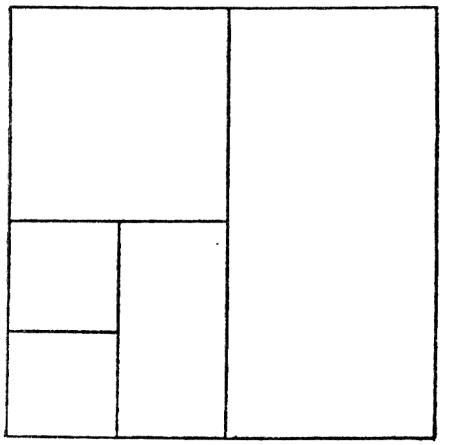
MINISTERUL EDUCAȚIEI ȘI ÎNVĂȚĂMÎNTULUI

Prof. dr. CONSTANTIN P. POPOVICI



TEORIA NUMERELOR

EDITURA DIDACTICĂ ȘI PEDAGOGICĂ, BUCUREȘTI
1973

Referent : Acad. Tiberiu Popoviciu

Redactor : Avram Pop
Tehnoredactor : Ana Țimpău
Coperta : Victor Wegeman

Prefață

În acest volum au fost cuprinse lecțiile de teoria numerelor pe care le-am ținut studenților, începînd din 1961, în cadrul unui curs special, al cărui conținut a suferit modificări, ajungînd la forma sub care este prezentat pentru publicare. Scopul acestor lecții era de a da demonstrațiile, cu mijloacele teoriei analitice elementare a numerelor, a legii asimptotice a distribuției numerelor prime și a teoremei lui Dirichlet referitoare la infinitatea numerelor prime. Din această cauză, aceste lecții au cuprins toate cele necesare din teoria elementară a numerelor și din teoria analitică elementară a numerelor.

Din teoria elementară a numerelor au fost tratate relația de congruență în inelul numerelor întregi și inelul numerelor m-*întregi, rezolvarea congruențelor și a sistemelor de congruențe cu o necunoscută, clase de resturi, teoremele lui Euler, Fermat și Wilson, rădăcini primitive, indici modulo* m, *funcții numerice, formule de inversare a sumelor, numărul numerelor prime, caractere modulo* m, *resturi pătratice, infinitatea numerelor prime. Constituite în primele 12 capitole, aceste lecții de teorie elementară a numerelor pot fi, privite ca formînd o parte independentă de restul volumului con-*

ținînd un ansamblu de cunoștințe pe care trebuie să le aibă orice matematician. Capitolul 12, referitor la infinitatea numerelor prime, cuprinde și cercetări originale ale autorului.

Din teoria analitică elementară a numerelor au fost expuse comportarea asimptotică și evaluări asimptotice ale cîtorva funcții numerice. Aceste cunoștințe au servit la demonstrarea legii asimptotice a distribuției numerelor prime și a teoremei lui Dirichlet referitoare la infinitatea numerelor prime. Metodele teoriei analitice elementare a numerelor sînt relativ simple și deosebit de eficace, motiv pentru care am ținut să le fac cunoscute studenților noștri, măcar în legătură cu cele două teoreme tratate în ultimele două capitole 15 și 16.

Acest volum, cel puțin în ceea ce privește teoria elementară a numerelor, poate servi drept o carte de referință și pentru profesorii de liceu care se pregătesc în vederea obținerii gradelor în învățămînt sau care conduc cercuri de matematică pentru elevi.

Autorul

Simboluri şi notaţii

Simbol sau notaţie	Semnificaţia lui
$\mid$	divide
$\nmid$	nu divide
&	şi
$\vee$	sau
$\Rightarrow$	implică
$\Leftrightarrow$	este echivalent cu (echivalenţă logică)
$\sim$	este echivalent cu (relaţie de echivalenţă)
$\nsim$	nu este echivalent cu
$\cong$	este asociat cu
$\ncong$	nu este asociat cu
$=$	este egal cu
$\neq$	nu este egal cu
$\equiv$	este congruent cu
$\not\equiv$	nu este congruent cu
$<$	este mai mic decît
$\leqslant$	este cel mult egal cu
$>$	este mai mare decît
$\geqslant$	este cel puţin egal cu
$+$	plus
$-$	minus
Σ	sumă
Π	produs

$\in$	aparţine
$\notin$	nu aparţine
φ	indicatorul lui Euler
$n!$	n-factorial
sign	signum
C_a	clasă de echivalenţă
$\hat{a}$	clasă de resturi
$\mathrm{ind}_g\, a$	indice al lui a modulo m în raport cu baza g
ind a	indice al lui a modulo m în raport cu baza g
mod m	modulo m
$\lvert a \rvert$	valoarea absolută a lui a
$[\alpha]$	partea întreagă a lui α
$\{\alpha\}$	partea fracţionară a lui α
(a, b)	cel mai mare divizor comun al lui a şi b
$[a, b]$	cel mai mic multiplu comun al lui a şi b
$\sum_{j=1}^{s} u(j)$	$u(1)+u(2)+\ldots+u(s)$
$\sum_{d\mid n} f(d)$	$f(d_1)+\ldots+f(d_t)$, unde $\{d_1, \ldots, d_t\}$ este mulţimea divizorilor pozitivi ai lui n
$\sum_{1\leqslant k\leqslant x} f(k)$	$f(1)+f(2)+\ldots+f([x])$
$\sum_{k\leqslant x} f(k)$	$f(1)+f(2)+\ldots+f([x])$
$\sum_{n>x} f(n)$	$n=\sum_{[x]+1}^{\infty} f(n)$
$\sum_{1\leqslant i_1<i_2<\ldots<i_s\leqslant r} f(i_1, i_2, \ldots, i_s)$	$f\left(i_1^{(1)}, i_2^{(1)}, \ldots, i_s^{(1)}\right)+f\left(i_1^{(2)}, i_2^{(2)}, \ldots, i_s^{(2)}\right)+\ldots+f\left(i_1^{(t)}, i_2^{(t)}, \ldots, i_s^{(t)}\right)$, unde $\{i_1^{(1)} i_2^{(1)} \ldots i_s^{(1)}, i_1^{(2)} i_2^{(2)} \ldots i_s^{(2)}, \ldots, i_1^{(t)} i_2^{(t)} \ldots i_s^{(t)}\}$ este mulţimea combinărilor $i_1 i_2 \ldots i_s$ de r elemente $1, 2, \ldots, r$ luate cîte s
$\prod_{j=1}^{r} u(j)$	$u(1)u(2)\ldots u(r)$
$\prod_{k\leqslant x} f(k)$	$f(1)f(2)\ldots f([x])$
τ	numărul divizorilor pozitivi
σ	suma divizorilor pozitivi
μ	funcţia lui Moebius

Λ	funcţia lui Mangoldt
log	logaritmul natura
ψ	funcţia pentru care $\psi(x)=\sum_{1\leqslant n\leqslant x} \Lambda(n)$
φ	funcţia pentru care $\varphi(x, r)$ este numărul numerelor naturale cel mult egale cu un număr real x şi care nu se divid cu nici unul din primele r numere prime pozitive
π	numărul numerelor prime
χ	caracter modulo m
$\left(\frac{a}{p}\right)$	simbolul lui Legendre
$\left(\frac{a}{m}\right)$	simbolul lui Jacobi
$f(x)=O(g(x))$	$f(x)$ este o mare de $g(x)$
$f(x)=o(g(x))$	$f(x)$ este o mic de $g(x)$
ϑ	funcţia pentru care $\vartheta(x)=\sum_{p\leqslant x} \log p$
R	funcţia pentru care $\psi(x)=x+R(x)$

Capitolul 1

RELAȚIA DE CONGRUENȚĂ

1.1. Definiția relației de congruență

Vom considera inelul numerelor întregi și în acest inel vom defini o relație care a căpătat numele de relație de congruență. Să reamintim ce se înțelege printr-un inel.

1.1.1. Definiția inelului

Un inel este o mulțime nevidă de elemente $a, b, \ldots$ *astfel încît*:

(0) *Fiecărei perechi de elemente* a, b *îi corespunde în mulțimea considerată un singur element numit sumă, notat* $a+b$, *și un singur element numit produs, notat* $a \cdot b$ *sau* ab.

Asocierea lui $a+b$ cu perechea a, b se numește *adunarea termenilor* a și b, iar asocierea lui ab cu perechea a, b se numește *înmulțirea factorilor* a și b.

(I) *Adunarea are următoarele proprietăți*:

(a) *asociativitate*: $(a+b)+c=a+(b+c)$,

(b) *comutativitate*: $a+b=b+a$,

(c) *existența soluției ecuației* $a+x=b$ *oricare ar fi* a *și* b.

Proprietățile adunării pot fi exprimate spunînd că față de adunare mulțimea considerată este *grup aditiv comutativ* sau *grup adiliv abelian*. În locul proprietății (c) pot figura alte două proprietăți :

(c1) *existența unui element, notat* 0, *numit element neutru la adunare* : $a+0=a$, *oricare ar fi* a,

(c2) *existența unui element notat* $-a$, *pentru fiecare element* a, *numit opusul lui* a : $a+(-a)=0$.

(II) *Înmulțirea are proprietatea*

(a) *asociativitate* : $(ab)c=a(bc)$.

(III) *Înmulțirea este distributivă față de adunare* :

$$\text{(a) } a(b+c)=ab+ac,$$

$$\text{(b) } (b+c)a=ba+ca.$$

Observație. Dacă și pentru înmulțire are loc proprietatea de comutativitate

$$ab=ba$$

inelul se numește comutativ. În cazul unor inele comutative există un element, notat 1, numit element neutru la înmulțire :

$$a\cdot 1=a.$$

Astfel de inele se numesc *inele comutative cu element unitate.*

Inelul numerelor întregi este inel comutativ cu element unitate.

Una dintre definițiile relației de congruență în inelul numerelor întregi o vom da cu ajutorul relației de divizibilitate definite în același inel.

1.1.2. Definiția relației de divizibilitate în inelul numerelor întregi

Un număr întreg b *divide un număr întreg* a *dacă există un număr întreg* c *astfel încît* $a=bc$.

Pentru a arăta că b divide pe a vom scrie $b|a$.

Relația de divizibilitate în inelul numerelor întregi are următoarele proprietăți :

(1, a) *reflexivitate* : $a|a$ *oricare ar fi numărul întreg* a,

(1, b) $-a|a$ *oricare ar fi numărul întreg* a.

(2) *tranzitivitate* : $a|b \,\&\, b|c \Rightarrow a|c$ (& trebuie citit „și“, iar $\Rightarrow$ *trebuie citit „implică“*).

(3) $a_1|b_1 \;\&\; a_2|b_2 \Rightarrow a_1a_2|b_1b_2$.

(4, a) $a|b \Rightarrow ac|bc$ *oricare ar fi numărul întreg* c,

(4, b) $ac|bc \;\&\; c\neq 0 \Rightarrow a|b$.

(5, a) $a|0$ *oricare ar fi numărul întreg* a,

(5, b) $\pm 1|a$ *oricare ar fi numărul întreg* a ($\pm 1|a$ trebuie înțeles în sensul că $1|a$ sau $-1|a$),

(5, c) $0|a \Rightarrow a=0$,

(5, d) $a|\pm 1 \Rightarrow a=\pm 1$ ($a=\pm 1$ trebuie înțeles în sensul că $a=1$ sau $a=-1$).

(6) $a|b \,\&\, b|a \Rightarrow b=\pm a$ ($b=\pm a$ trebuie înțeles în sensul că $b=a$ sau $b=-a$).

(7, a) $a|b_1 \,\&\, a|b_2 \Rightarrow a|b_1 \pm b_2$ ($a|b_1 \pm b_2$ trebuie înțeles în sensul că $a|b_1+b_2$ sau $a|b_1-b_2$),

(7, b) $a|b \Rightarrow a|cb$ *oricare ar fi numărul întreg* c,

(7, c) $a|b_1 \,\&\, a|b_2 \Rightarrow a|c_1b_1+c_2b_2$ *oricare ar fi numerele întregi* c_1 *și* c_2.

(8) $a|b \,\&\, b\neq 0 \Rightarrow |a| \leqslant |b|$.

Relația de divizibilitate în inelul numerelor întregi permite definirea relației de asociere în inelul numerelor întregi.

1.1.3. Definiția relației de asociere în inelul numerelor întregi

(a) *Numerele întregi* a *și* b *sînt asociate dacă* $a|b \,\&\, b|a$.

Pentru a arăta că numerele întregi a și b sînt asociate, vom scrie

$$a \cong b.$$

Putem defini relația de asociere în inelul numerelor întregi în felul următor :

(b) *Numerele întregi* a *și* b *sînt asociate dacă* $b=\pm a$.

(c) *Numerele întregi* a *și* b *sînt asociate dacă* $|a|=|b|$.

(d) *Numerele întregi* a *și* b *sînt asociate dacă* $|a| \leqslant |b| \,\&\, |b| \leqslant |a|$.

Aceste patru definiții sînt echivalente.

Relația de asociere în inelul numerelor întregi are următoarele proprietăți :

(1) *reflexivitate* : $a \cong a$,

(2) *simetrie* : $a \cong b \Rightarrow b \cong a$,

(3) *tranzitivitate* : $a \cong b \,\&\, b \cong c \Rightarrow a \cong c$.

Avînd aceste trei proprietăți relația de asociere în inelul numerelor întregi este *relație de echivalență* în inelul numerelor întregi.

Observație. Din definiția (b) a relației de asociere în inelul numerelor întregi se constată că numărul întreg a este asociat numai cu a și $-a$. Deci numerele întregi asociate cu un număr întreg a se obțin din a prin înmulțire cu unitățile inelului numerelor întregi, deoarece $a=1\cdot a$ și $-a=(-1)\cdot a$, prin unitățile inelului numerelor întregi înțelegîndu-se acele numere întregi care divid pe 1 și care sînt numai 1 și -1 datorită proprietății (5, d, a relației de divizibilitate în inelul numerelor întregi.

După această parte introductivă putem da definiția relației de congruență în inelul numerelor întregi.

1.2. Prima definiție a relației de congruență în inelul numerelor întregi

Două numere întregi a și b sînt congruente modulo m, unde m este un număr întreg, dacă :

$$m|a-b.$$

Pentru a arăta că numerele întregi a și b sînt congruente modulo m, se scrie

$$a\equiv b(\text{mod } m).$$

Numărul întreg m se numește *modulul* relației de congruență.

Relația de congruență, în inelul numerelor întregi, are următoarele proprietăți :

(1) *reflexivitate* : $a\equiv a$ (mod m), *oricare ar fi numărul întreg a.*

(2) *simetrie* : $a\equiv b$ (mod m)$\Rightarrow b\equiv a$ (mod m).

(3) *tranzitivitate* : $a\equiv b$ (mod m)$\&\, b\equiv c$ (mod m)$\Rightarrow a\equiv c$ (mod m).

(4, a) $a\equiv b$ (mod m)$\&\, c\equiv d$ (mod m)$\Rightarrow a+c\equiv b+d$ (mod m),

(4, b) $a\equiv b$ (mod m)$\&\, c\equiv d$ (mod m)$\Rightarrow a-c\equiv b-d$ (mod m),

(4, c) $a\equiv b+c$ (mod m)$\Rightarrow a-c\equiv b$ (mod m).

(5, a) $a\equiv b$ (mod m)$\&\, c\equiv d$ (mod m)$\Rightarrow ac\equiv bd$ (mod m),

(5, b) $a\equiv b$ (mod m)$\Rightarrow ac\equiv bc$ (mod mc), *oricare ar fi numărul întreg c,*

(5, c) $ac\equiv bc$ (mod mc)$\&\, c\neq 0\Rightarrow a\equiv b$ (mod m),

(5, d) $a\equiv b$ (mod m)$\Rightarrow ac\equiv bc$ (mod m), *oricare ar fi numărul întreg c,*

(5, e) $ac\equiv bc$ (mod m)$\&\,(c,\ m)\cong 1\Rightarrow a\equiv b$ (mod m).

Prin $(c,\ m)$ a fost notat cel mai mare divizor comun al numerelor întregi c și m.

(6, a) $a\equiv b$ (mod 0)$\Leftrightarrow a=b$,

($\Leftrightarrow$ trebuie citit, „este echivalent cu")

(6, b) $a\equiv b$ (mod ± 1) *oricare ar fi numerele întregi a și b* ($a\equiv b$ (mod ± 1) trebuie înțeles în sensul că $a\equiv b$ (mod 1) *sau* $a\equiv b$ (mod -1)).

(7) $a\equiv b$ (mod m)$\&\, n|m\Rightarrow a\equiv b$ (mod n).

(8, a) $a\equiv b$ (mod m)$\&\,(a,\ m)\cong d\Rightarrow(b,\ m)\cong d$,

(8, b) $a\equiv b$ (mod m)$\&\, m|a\Rightarrow m|b$,

(8, c) $a\equiv b$ (mod m)$\&\,(a,\ m)\cong 1\Rightarrow(b,\ m)\cong 1$.

Aceste proprietăți ale relației de congruență în inelul numerelor întregi se demonstrează în felul următor :

(1) $m|0$ oricare ar fi numărul întreg m. Apoi $a-a=0$, oricare ar fi numărul întreg a, deci $m|a-a$, de unde $a\equiv a$ (mod m).

(2) $a\equiv b$ (mod m) înseamnă $m|a-b$. Deci $m|(-1)(a-b)$, de unde $m|b-a$ sau $b\equiv a$ (mod m).

(3) $a\equiv b$ (mod m) înseamnă $m|a-b$, iar $b\equiv c$ (mod m) înseamnă $m|b-c$. Deci $m|(a-b)+(b-c)$, de unde $m|a-c$ sau $a\equiv c$ (mod m).

(4, a) $a\equiv b$ (mod m) înseamnă $m|a-b$, iar $c\equiv d$ (mod m) înseamnă $m|c-d$. Deci $m|(a-b)+(c-d)$ de unde $m|(a+c)-(b+d)$ sau $a+c\equiv b+d$ (mod m).

(4, b) $a\equiv b$ (mod m) înseamnă $m|a-b$, iar $c\equiv d$ (mod m) înseamnă $m|c-d$. Deci $m|(a-b)-(c-d)$, de unde $m|(a-c)-(b-d)$ sau $a-c\equiv b-d$ (mod m).

(4, c) $a\equiv b+c$ (mod m) înseamnă $m|a-(b+c)$. Deci $m|(a-c)-b$ sau $a-c\equiv b$ (mod m).

(5, a) $a\equiv b$ (mod m) înseamnă $m|a-b$, iar $c\equiv d$ (mod m) înseamnă $m|c-d$. Deci $m|c(a-b)+b(c-d)$ de unde $m|ac-bd$ sau $ac\equiv bd$ (mod m).

(5, b) $a\equiv b$ (mod m) înseamnă $m|a-b$. Deci $mc|(a-b)c$ oricare ar fi numărul întreg c. Rezultă $mc|ac-bc$ sau $ac\equiv bc$ (mod mc) oricare ar fi numărul întreg c.

(5, c) $ac\equiv bc$ (mod m) înseamnă $mc|ac-bc$. Deci $mc|(a-b)c$. Dacă $c\neq 0$ rezultă $m|a-b$ sau $a\equiv b$ (mod m).

(5, d) $a\equiv b$ (mod m) înseamnă $m|a-b$. Deci $m|c(a-b)$ oricare ar fi numărul întreg c. Rezultă $m|ac-bc$ sau $ac\equiv bc$ (mod m) oricare ar fi numărul întreg c.

(5, e) $ac\equiv bc$ (mod m) înseamnă $m|ac-bc$. Deci $m|(a-b)c$. Dacă $(c,\ m)\cong 1$ rezultă $m|a-b$ sau $a\equiv b$ (mod m).

(6, a) $a\equiv b$ (mod 0) înseamnă $0|a-b$. Dar $0|a-b\Leftrightarrow a=b$. În adevăr, dacă $0|a-b$ rezultă $a-b=0$ sau $a=b$. Dacă $a=b$ rezultă $a-b=0$ și din cauză că $0|0$ se obține $0|a-b$ sau $a\equiv b$ (mod m).

(6, b) Oricare ar fi numerele întregi a, b, diferența $a-b$ este un număr întreg, deci $1|a-b$ sau $a\equiv b \pmod 1$ ori $-1|a-b$ sau $a\equiv b \pmod{-1}$.

(7) $a\equiv b \pmod m$ înseamnă $m|a-b$. Apoi $n|m \& m|a-b \Rightarrow n|a-b$, deci $a\equiv b \pmod n$.

(8, a) $a\equiv b \pmod m$ înseamnă $m|a-b$. Deci există un număr întreg k astfel încît $a-b=mk$. Vom nota $d\cong(a, m)$, $D\cong(b, m)$ și vom demonstra că $D\cong d$, adică $d\cong(b, m)$. Avem $d|a$, $d|m$, deci $d|1\cdot a+(-k)m$, de unde $d|b$, deoarece $b=a-mk$. Din $d|b$, $d|m$ rezultă $d|D$, deoarece $d\cong(b, m)$. Avem și $D|b$, și $D|m$, deci $D|1\cdot b+k\cdot m$, de unde $D|a$, deoarece $a=b+mk$. Din $D|a$, $D|m$ rezultă $D|d$, deoarece $D\cong(a, m)$. Din $d|D$, $D|d$ rezultă $D\cong d$.

(8, b) $m|a\Rightarrow m\cong(a, m)$. Deci $a\equiv b \pmod m \& m|a\Rightarrow m\cong(b, m)$, conform proprietății (8, a) a relației de congruență în inelul numerelor întregi, de unde $m|b$.

(8, c) Această proprietate este un caz particular al proprietății (8, a) a relației de congruență în inelul numerelor întregi în cazul cînd $d\cong 1$.

1.3. A doua definiție a relației de congruență în inelul numerelor întregi

Două numere întregi a și b sînt congruente modulo m, unde m este un număr întreg diferit de zero, dacă există numere întregi q_1, q_2, r astfel încît

$$a=mq_1+r,\ 0\leqslant r<|m|,$$

$$b=mq_2+r,\ 0\leqslant r<|m|.$$

Observație. Fiind date numerele întregi a și m, $m\neq 0$, a găsi numerele întregi q_1 și r astfel încît

$$a=mq_1+r,\ 0\leqslant r<|m|$$

înseamnă a aplica teorema împărțirii întregi numerelor întregi a și m, $m\neq 0$. La aplicarea teoremei împărțirii întregi numerelor întregi a și m, împărțitorul m trebuie să fie diferit de zero. Din această cauză cea de-a doua definiție a relației de congruență

în inelul numerelor întregi nu poate fi utilizată în cazul cînd modulul relației de congruență este egal cu zero. Am convenit ca numărul întreg m să fie numit și de această dată *modulul* relației de congruență. Vom completa cea de-a doua definiție a relației de congruență în inelul numerelor întregi, în cazul cînd modulul este egal cu zero, spunînd că relația de congruență în inelul numerelor întregi în cazul cînd modulul este egal cu zero este relația de egalitate în inelul numerelor întregi. Este indicat să facem această completare, deoarece în cazul primei definiții a relației de congruență în inelul numerelor întregi avem proprietatea (6, a) $a\equiv b \pmod 0 \Leftrightarrow a=b$ și mai ales, după cum vom demonstra, cele două definiții ale relației de congruență în inelul numerelor întregi în cazul cînd modulul este diferit de zero sînt echivalente.

Teoremă. *Cele două definiții ale relației de congruență în inelul numerelor întregi sînt echivalente în cazul în care modulul relației de congruență este diferit de zero.*

Demonstrație. Să admitem că două numere întregi a și b sînt congruente modulo m după prima definiție. În acest caz avem $m|a-b$, deci există un număr întreg c astfel încît $a-b=mc$. Aplicînd teorema împărțirii întregi lui b și m, ceea ce putem face, deoarece am presupus că $m\neq 0$, găsim două numere întregi q și r astfel încît

$$b=mq+r,\ 0\leqslant r<|m|.$$

Din cauză că $a-b=mc$ obținem

$$a=m(c+q)+r,\ 0\leqslant r<|m|,$$

ceea ce constituie aplicarea teoremei împărțirii întregi lui a și m, deoarece cîtul și restul din teorema împărțirii întregi fiind unice, nu contează modul cum ajungem la relațiile care exprimă teorema împărțirii întregi. Am ajuns la concluzia că cele două numere întregi a și b sînt congruente modulo m și după a doua definiție.

Să admitem că două numere întregi a și b sînt congruente modulo m după a doua definiție. În acest caz există numere întregi q_1, q_2, r astfel încît

$$a=mq_1+r,\ 0\leqslant r<|m|,$$

$$b=mq_2+r,\ 0\leqslant r<|m|.$$

Scăzînd membru cu membru aceste două relații, obținem

$$a-b=m(q_1-q_2),$$

deci $m|a-b$, deoarece q_1-q_2 este un număr întreg, adică numerele întregi a și b sînt congruente modulo m și după prima definiție.

Observație. Cele două definiții ale relației de congruență în inelul numerelor întregi fiind echivalente, relația de congruență în inelul numerelor întregi, dată după a doua definiție, o vom nota la fel cum am notat relația de congruență în inelul numerelor întregi, dată după prima definiție, adică prin

$$a\equiv b \pmod m.$$

1.4. Utilizarea relației de congruență în inelul numerelor întregi la rezolvarea problemelor de divizibilitate

Vom arăta cum folosind proprietățile relației de congruență în inelul numerelor întregi putem rezolva fără prea mult efort diverse probleme de divizibilitate.

Exemplul 1. Să se arate că $17|7^{201}+2\cdot 3^{100}\cdot 5^{101}$.

Avem $7^{201}+2\cdot 3^{100}\cdot 5^{101}=(7^2)^{100}\cdot 7+2(3\cdot 5)^{100}\cdot 5=49^{100}\cdot 7+2\cdot 15^{100}5$. Însă $49\equiv 15 \pmod{17}$, deci $49^{100}\equiv 15^{100} \pmod{17}$, așadar $7^{201}+2\cdot 3^{100}\cdot 5^{101}\equiv 15^{100}\cdot 7+2\cdot 15^{100}\cdot 5\equiv 15^{100}(7+2\cdot 5)\equiv 15^{100}\cdot 17 \pmod{17}$.

Deci

$7^{201}+2\cdot 3^{100}\cdot 5^{101}\equiv 15^{100}\cdot 17 \pmod{17}$

și deoarece $17|15^{100}\cdot 17$ înseamnă că $17|7^{201}+2\cdot 3^{100}\cdot 5^{101}$.

Exemplul 2. Să se arate că $641|2^{2^5}+1$.

Se observă că $641=640+1=5\cdot 2^7+1$ și $641=625+16=5^4+2^4$ deci $5\cdot 2^7\equiv -1 \pmod{641}$ deoarece $641|5\cdot 2^7-(-1)$ avînd $641=5\cdot 2^7+1$ și $5^4\equiv -2^4 \pmod{641}$, deoarece $641|5^4-(-2^4)$ avînd $641=5^4+2^4$. Din $5\cdot 2^7\equiv -1 \pmod{641}$ deducem $5^4\cdot 2^{28}\equiv 1 \pmod{641}$ și din $5^4\equiv -2^4 \pmod{641}$ deducem $5^4\cdot 2^{28}\equiv -2^{32} \pmod{641}$, deci $1\equiv -2^{32} \pmod{641}$ sau $2^{2^5}+1\equiv 0 \pmod{641}$. Deoarece $641|0$ rezultă $641|2^{2^5}+1$.

Exemplul 3. Să se calculeze restul împărțirii dintre 547^{79} și 19, împărțitorul fiind 19.

Dacă r este un număr întreg care verifică inegalitățile

$$0\leqslant r<19,$$

iar 547^{79} este congruent cu r modulo 19, atunci r este restul împărțirii dintre 547^{79} și 19, împărțitorul fiind 19. Într-adevăr dacă

$$547^{79}\equiv r \pmod{19}$$

atunci $19|547^{79}-r$, deci există un număr întreg q astfel încît $547^{79}-r=19q$. Deci

$$547^{79}=19q+r,\ 0\leqslant r<19.$$

Dar aceasta înseamnă că r este restul împărțirii dintre 547^{79} și 19, împărțitorul fiind 19.

Există un număr întreg r astfel încît $0\leqslant r<19$ și

$$547^{79}\equiv r \pmod{19}$$

deoarece aplicînd teorema împărțirii întregi lui 547^{79} și 19, împărțitorul fiind 19, găsim numere întregi q și r astfel încît

$$547^{79}=19q+r,\ 0\leqslant r<19,$$

deci $547^{79}-r=19q$ sau $19|547^{79}-r$ de unde $547^{79}\equiv r \pmod{19}$.

Pentru a determina numărul întreg r de mai sus, vom face calculele în modul următor:

Prin aplicarea teoremei împărțirii întregi numerelor întregi 547 și 19, împărțitorul fiind 19, obținem

$$547=19\cdot 28+15,$$

deci $547\equiv 15 \pmod{19}$ din cauză că $547-15=19\cdot 28$, adică $19|547-15$. Așadar

$$547^{79}\equiv 15^{79} \pmod{19}.$$

Din cauză că $15\equiv -4 \pmod{19}$ mai putem scrie

$$547^{79}\equiv (-4)^{79}\equiv -2^{158} \pmod{19}.$$

Dar $2^9\equiv (2^3)^3\equiv 512\equiv -1 \pmod{19}$, deci dacă vom scrie $158=9\cdot 17+5$ vom obține

$$547^{79}\equiv -2^{158}\equiv -(2^9)^{17}2^5\equiv -(-1)^{17}2^5\equiv 2^5\equiv 32\equiv 13 \pmod{19}$$

deci restul împărțirii dintre 547^{79} și 19, împărțitorul fiind 19, este 13.

Capitolul 2

REZOLVAREA CONGRUENȚELOR ȘI A SISTEMELOR DE CONGRUENȚE CU O NECUNOSCUTĂ

2.1. Rezolvarea congruenței de gradul întîi cu o necunoscută

Congruența $ax \equiv b \pmod m$, unde a, b sînt numere întregi, se numește *congruență de gradul întîi* cu o necunoscută x. A rezolva această congruență înseamnă a găsi un număr întreg c, numit *soluție* a congruenței considerate, astfel încît $ac \equiv b \pmod m$. Două soluții se consideră *identice* dacă sînt congruente modulo m și *distincte* dacă nu sînt congruente modulo m. Se consideră identice două soluții ale congruenței $ax \equiv b \pmod m$ care sînt congruente modulo m, deoarece dacă x_0 este o soluție a congruenței $ax \equiv b \pmod m$, atunci orice număr întreg x_1 astfel încît $x_1 \equiv x_0 \pmod m$ este o soluție a aceleiași congruențe, pentru că din $x_1 \equiv x_0 \pmod m$ se deduce $ax_1 \equiv ax_0 \pmod m$, deci $ax_1 \equiv b \pmod m$.

Condițiile în care congruența $ax \equiv b \pmod m$ are soluții sînt date în următoarea:

Teoremă. *Condiția necesară și suficientă ca congruența*

$$ax \equiv b \pmod m$$

să aibă soluții este ca $d \mid b$, *unde* $d \cong (a, b)$.

Demonstrație. Condiția necesară și suficientă ca congruența $ax \equiv b \pmod m$ să aibă soluții este ca ecuația diofantică $ax + my = b$

să aibă soluții. Într-adevăr, congruența $ax \equiv b \pmod m$ admite soluții dacă și numai dacă există un număr întreg x_0 astfel încît $ax_0 \equiv b \pmod m$ sau $m \mid ax_0 - b$. Această relație are loc dacă și numai dacă există un număr întreg $-y_0$ astfel încît $ax_0 - b = m(-y_0)$ sau $ax_0 + my_0 = b$. Deci ecuația diofantică $ax + my = b$ admite soluții dacă și numai dacă congruența $ax \equiv b \pmod m$ admite soluții. Dar condiția necesară și suficientă ca ecuația diofantică $ax + my = b$ să aibă soluții este ca $d \mid b$, unde $d \cong (a, m)$.

Observație. La rezolvarea congruenței

$$ax \equiv b \pmod m,$$

în cazul în care această congruență are soluții, întîlnim mai multe cazuri.

Astfel putem avea $m = 0$. Atunci congruența $ax \equiv b \pmod m$ se transformă în ecuația $ax = b$, iar $d \cong (a, m) \cong (a, 0) \cong a$. Dacă $d \neq 0$, deci $a \neq 0$, avem $a \mid b$ din $d \mid b$, deoarece am presupus că congruența $ax \equiv b \pmod m$ are soluții. Deci $x = b : a$ este în acest caz singurul număr întreg care este soluție a congruenței $ax \equiv b \pmod m$. Dacă $d = 0$, deci $a = 0$, avem și $b = 0$, ceeace se deduce din $d \mid b$, deoarece am presupus că congruența $ax \equiv b \pmod m$ are soluții. Atunci congruența $ax \equiv b \pmod m$ se transformă în ecuația $0x = 0$ care are ca soluție orice număr întreg.

Mai putem avea $m \neq 0$. În acest caz soluțiile congruenței $ax \equiv b \pmod m$ se obțin după cum urmează.

Teoremă. *Dacă* x_0 *este o soluție a congruenței*

$$ax \equiv b \pmod m,$$

în cazul în care $m \neq 0$, *atunci* $x_0 + vr$ *cu* $v = m : d$ *și* $0 \leqslant r < d$, r *fiind un număr întreg, sînt* d *soluții distincte ale congruenței considerate, care are numai* d *soluții distincte, unde* $d \cong (a, m)$, $d > 0$.

Demonstrație. Dacă $m \neq 0$ și x_0 este o soluție a congruenței $ax \equiv b \pmod m$, atunci $ax_0 \equiv b \pmod m$, ceea ce înseamnă $m \mid ax_0 - b$, deci există un număr întreg $-y_0$ astfel încît $ax_0 - b = m(-y_0)$ sau $ax_0 + my_0 = b$. Atunci soluțiile ecuației diofantice $ax + my = b$ sînt $x = x_0 + vt$, $y = y_0 - ut$, unde $u = a : d$, $v = m : d$, iar t este orice număr întreg. Aplicînd teorema împărțirii întregi lui t și d, acest lucru fiind posibil, deoarece $d \neq 0$, ceea ce rezultă din $m \neq 0$ și $d \cong (a, m)$, avem $t = qd + r$, unde $0 \leqslant r < d$. Avem deci $x = x_0 + v(qd + r) = x_0 + vr + (vd)q = x_0 + vr + mq$. Deci $x \equiv x_0 + vr \pmod m$. Dacă $r_1 \neq r_2$ atunci $x_0 + vr_1 \not\equiv x_0 + vr_2 \pmod m$, deoarece în

caz contrar, din $x_0+vr_1\equiv x_0+vr_2 \pmod m$ am deduce $vr_1\equiv vr_2 \pmod m$ sau $v(r_1-r_2)\equiv 0 \pmod{vd}$ sau $r_1-r_2\equiv 0 \pmod d$, pentru că $v\neq 0$, ceea ce rezultă din $m\neq 0$ și $v=m:d$. Dar $r_1-r_2\equiv 0 \pmod d$ înseamnă $d\mid r_1-r_2$, deci există un număr întreg q astfel încît $r_1-r_2=dq$, de unde $r_1=dq+r_2$, în care $0\leqslant r_1<d$, $0\leqslant r_2<d$. Scriind pe r_1 sub forma $r_1=d\cdot 0+r_1$ deducem $r_1=r_2$, deoarece restul împărțirii numărului întreg r_1 prin d este unic. Am ajuns la o contradicție care dovedește că x_0+vr cu $0\leqslant r<d$ sînt d soluții distincte ale congruenței $ax\equiv b \pmod m$ și în același timp am arătat că această congruență are numai d soluții distincte, deoarece am arătat că orice soluție a congruenței $ax\equiv b \pmod m$ este congruentă măcar cu unul dintre numerele întregi x_0+vr cu $0\leqslant r<d$.

Observație. Dacă $(a,m)\cong 1$ atunci congruența $ax\equiv b \pmod m$ are o singură soluție, avînd $1\mid b$, numărul soluțiilor fiind dat de 1 care este (a, m).

2.2. Rezolvarea sistemelor de congruențe de gradul întîi cu o necunoscută

Teoremă. *Condiția necesară și suficientă ca sistemul de congruențe*

$$\begin{aligned} &x\equiv a_1 \pmod{m_1},\\ &\cdots\cdots\cdots\cdots\\ &x\equiv a_s \pmod{m_s}, \end{aligned}$$

unde $m_1\neq 0, \ldots, m_s\neq 0$, *să admită soluții este ca*

$$M_j(a_j-a_i)\equiv 0 \pmod{m_i},\ (i,j=1,\ldots,s),$$

unde $M_jm_j=m$ $(j=1,\ldots,s)$ m *fiind cel mai mic multiplu comun al lui* $m_1,\ldots,m_s$.

În cazul în care sistemul de congruențe de mai sus admite soluții, atunci acestea sînt numai numerele întregi congruente modulo m *cu numărul întreg*

$$x_0=\sum_{j=1}^{s} M_ja_jb_j$$

numerele întregi b_j *fiind definite prin relația*

$$b_1M_1+b_2M_2+\ldots+b_sM_s=1.$$

Demonstrație. Admitem că sistemul de congruențe

$$\begin{aligned} &x\equiv a_1 \pmod{m_1},\\ &\cdots\cdots\cdots\cdots\\ &x\equiv a_s \pmod{m_s} \end{aligned}$$

admite o soluție care este un număr întreg x. Obținem

$$M_jx\equiv M_ja_j \pmod{M_jm_j},\ (j=1,\ldots,s),$$
$$M_jx\equiv M_ja_i \pmod{M_jm_i},\ (i,\ j=1,\ldots,s).$$

Însă $M_jm_j=m=M_im_i$, deci $m_i\mid M_jm_j$, deci

$$M_jx\equiv M_ja_j \pmod{m_i},\ (i,\ j=1,\ldots,s),$$
$$M_jx\equiv M_ja_i \pmod{m_i},\ (i,\ j=1,\ldots,s),$$

deci

$$M_j(a_j-a_i)\equiv 0 \pmod{m_i},\ (i,\ j=1,\ldots,s)$$

este o condiție necesară ca sistemul de congruențe considerat să admită soluții.

Să arătăm că această condiție este și suficientă. Pentru aceasta vom arăta că x_0 este o soluție a sistemului de congruențe de mai sus, dacă $M_j(a_j-a_i)\equiv 0 \pmod{m_i}$, $(i,\ j=1,\ldots,s)$. Avem

$$x_0=\sum_{j=1}^{s} M_ja_jb_j=M_ia_ib_i+\sum_{\substack{j=1\\ j\neq i}}^{s} M_ja_jb_j=$$

$$=a_i\left(1-\sum_{\substack{j=1\\ j\neq i}}^{s} M_jb_j\right)+\sum_{\substack{j=1\\ j\neq i}}^{s} M_ja_jb_j=$$

$$=a_i+\sum_{\substack{j=1\\ j\neq i}}^{s} M_j(a_j-a_i)b_j=a_i+\sum_{j=1}^{s} M_j(a_j-a_i)b_j.$$

Dar dacă $M_j(a_j-a_i)\equiv 0 \pmod{m_i}$, $(i,\ j=1,\ldots,s)$, atunci

$$x_0\equiv a_i \pmod{m_i},\ (i=1,\ldots,s)$$

deci condiția $M_j(a_j-a_i)\equiv 0 \pmod{m_i}$, $(i,\ j=1,\ldots,s)$ este și suficientă ca sistemul de congruențe considerat să admită soluții,

deoarece în cazul în care această condiție este satisfăcută, numărul întreg x_0 este o soluție a sistemului de congruențe considerat.

Să arătăm acum că orice număr întreg care este o soluție a sistemului de congruențe considerat este congruent cu x_0 modulo m.

Într-adevăr, pentru orice soluție x a sistemului de congruențe considerat, în cazul în care acesta are o soluție, avem

$$M_j x \equiv M_j a_j \pmod{M_j m_j}, \quad (j=1, \ldots, s).$$

Numerele M_j $(j=1, \ldots, s)$ sînt prime între ele, deoarece $M_j m_j = m$ $(j=1, \ldots, s)$, m fiind cel mai mic multiplu comun al lui $m_1, \ldots, m_s$, deci există numere întregi b_j $(j=1, \ldots, s)$ astfel încît să avem

$$b_1 M_1 + b_2 M_2 + \ldots + b_s M_s = 1,$$

deci

$$b_j M_j x \equiv M_j a_j b_j \pmod{m}$$

deci

$$\left(\sum_{j=1}^{s} b_j M_j\right) x \equiv \sum_{j=1}^{s} M_j a_j b_j \pmod{m},$$

deci

$$x \equiv x_0 \pmod{m}$$

și în felul acesta am arătat nu numai că orice soluție a sistemului de congruențe considerat este congruentă cu x_0 modulo m, dar am determinat și modul de calcul al soluției x_0.

Consecință. *Dacă numerele $m_1, \ldots, m_s$ sînt prime două cîte două, dar și $m_1 \neq 0, \ldots, m_s \neq 0$, atunci sistemul de congruențe*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ &\cdots\cdots\cdots\cdots \\ x &\equiv a_s \pmod{m_s} \end{aligned}$$

admite soluții.

Într-adevăr, dacă $m_1, \ldots, m_s$ sînt prime două cîte două, iar $m_1 \neq 0, \ldots, m_s \neq 0$, atunci $m = m_1 \ldots m_s$ și deci $M_i = m_1 \ldots m_{i-1} \cdot m_{i+1} \ldots m_s$. Deci $m_i \mid M_j$ dacă $i \neq j$. Dar atunci condițiile

$$M_j(a_j - a_i) \equiv 0 \pmod{m_i}, \quad (i, j=1, \ldots, s)$$

sînt îndeplinite.

Exemplul 1. Sistemul de congruențe

$$x \equiv 4 \pmod 5,$$

$$x \equiv 6 \pmod 7$$

admite soluții, deoarece modulii 5 și 7 sînt primi între ei. Avem $[5, 7] \cong 35$. Punînd $m_1=5$, $m_2=7$ obținem $m_1 M_1 = m_2 M_2 = 35$, deci $M_1=7$, $M_2=5$. Trebuie să determinăm o pereche de numere întregi b_1, b_2 pentru care

$$b_1 7 + b_2 5 = 1.$$

Putem lua $b_1=-2$, $b_2=3$. Soluția sistemului de congruențe considerat este

$$x \equiv 7 \cdot 4 \cdot (-2) + 5 \cdot 6 \cdot 3 \pmod{35}$$

adică

$$x \equiv -56 + 90 \equiv 34 \pmod{35}.$$

Exemplul 2. Sistemul de congruențe

$$x \equiv 4 \pmod{15},$$

$$x \equiv 6 \pmod{21}$$

nu admite soluții, deoarece $m \cong [15, 21] \cong 105$, $M_1=7$, $M_2=3$ și

$$M_1(4-6) = 7(-2) \not\equiv 0 \pmod{21}.$$

Avem și

$$M_2(6-4) = 3(2) \not\equiv 0 \pmod{15}.$$

2.3. Congruențe în raport cu un modul prim

Vom considera congruențele de forma

$$f(x) \equiv 0 \pmod p,$$

unde p este un număr prim, iar $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$, a_n, $a_{n-1}, \ldots, a_0$ fiind numere întregi.

Pentru asemenea congruențe are importanță formula de interpolare a lui Newton care este formulată în următoarea :

Teoremă. *Fiind date n numere întregi* $x_1, x_2, \ldots, x_n$ *există* $n+1$ *numere întregi* $c_n, c_{n-1}, \ldots, c_0$ *astfel încît să avem*

$$f(x)=c_n(x-x_1)\ (x-x_2)\ldots(x-x_n)+$$
$$+c_{n-1}(x-x_1)\ (x-x_2)\ldots(x-x_{n-1})+$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$+c_1(x-x_1)+$$
$$+c_0.$$

Demonstrație. Presupunînd existența numerelor întregi c_n, $c_{n-1}, \ldots, c_0$ astfel încît $f(x)$ să poată fi scris sub forma dată de formula de interpolare a lui Newton și luînd

$$(x-x_1)\ (x-x_2)\ldots(x-x_i)=x^i+b_{i-1,i}x^{i-1}+\ldots+b_{0,i},$$

unde $b_{i-1,i}, \ldots, b_{0,i}$ sînt numere întregi, obținem

$$f(x)=c_n(x^n+b_{n-1,n}x^{n-1}+\ldots+b_{0,n})+c_{n-1}(x^{n-1}+$$
$$+b_{n-2,n-1}x^{n-2}+\ldots+b_{0,n-1})+\ldots+c_1(x+b_{0,1})+c_0=$$
$$=c_nx^n+(c_{n-1}+b_{n-1,n}c_n)x^{n-1}+\ldots+(c_0+c_1b_{0,1}+\ldots+$$
$$+c_{n-1}b_{0,n-1}+c_nb_{0,n}).$$

Deci

$$a_n=c_n,$$
$$a_{n-1}=c_{n-1}+b_{n-1,n}c_n,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$a_0=c_0+c_1b_{0,1}+\ldots+c_{n-1}b_{0,n-1}+c_nb_{0,n}$$

din cauză că

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0.$$

Constatăm că putem determina numerele întregi $c_n, c_{n-1}, \ldots, c_0$ astfel încît $a_n, a_{n-1}, \ldots, a_0$ să fie date prin relațiile de mai sus, deoarece este suficient să luăm

$$c_n=a_n,$$
$$c_{n-1}=a_{n-1}-b_{n-1,n}c_n,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$c_0=a_0-(c_1b_{0,1}+\ldots+c_{n-1}b_{0,n-1}+c_nb_{0,n}).$$

Înlocuind în $f(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0$ pe $a_n, a_{n-1}\ldots, a_1$, a_0 cu exprimările lor în care intervin $c_n, c_{n-1}, \ldots, c_0$ și refăcînd calculele în sens invers, dovedim că $f(x)$ se scrie sub forma dată de formula de interpolare a lui Newton.

Observație. Ca și la congruențele de gradul întîi înțelegem prin soluție a congruenței $f(x)\equiv 0 \pmod p$, unde $f(x)$ este de forma de mai sus, orice număr întreg c astfel încît $f(c)\equiv 0 \pmod p$. Două soluții se consideră identice dacă sînt congruente modulo p și distincte dacă nu sînt congruente modulo p. Se consideră identice două soluții ale congruenței $f(x)\equiv 0 \pmod p$ care sînt congruente modulo p, deoarece dacă x_0 este o soluție a congruenței $f(x)\equiv 0 \pmod p$, atunci orice număr întreg x_1 astfel încît $x_1\equiv x_0 \pmod p$ este o soluție a aceleiași congruențe, pentru că din $x_1\equiv x_0 \pmod p$ se deduce $f(x_1)\equiv f(x_0) \pmod p$, deci $f(x_1)\equiv 0 \pmod p$.

Teoremă. *Dacă congruența*

$$f(x)\equiv 0 \pmod p,$$

unde p *este un număr prim,* $f(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_0$, a_n, $a_{n-1}, \ldots, a_0$ *fiind numere întregi, are mai mult de* n *soluții distincte, atunci coeficienții* $a_n, a_{n-1}, \ldots, a_0$ *se divid cu* p.

Demonstrație. Să notăm cu $x_1, x_2, \ldots, x_{n+1}$, $n+1$ soluții distincte ale congruenței de mai sus, presupunînd că această congruență are mai mult de n soluții distincte. Atunci există numere întregi $c_n, c_{n-1}, \ldots, c_0$ ca să putem scrie

$$f(x)=c_n(x-x_1)\ (x-x_2)\ldots(x-x_n)+$$
$$+c_{n-1}\,(x-x_1)\ (x-x_2)\ldots(x-x_{n-1})+$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$+c_1(x-x_1)+$$
$$+c_0.$$

Din cauză că $f(x_1)\equiv 0 \pmod p$, rezultă $c_0\equiv 0 \pmod p$, deci $p\mid c_0$. Presupunem, datorită raționamentului prin inducție completă, că $p\mid c_0$, $p\mid c_1, \ldots, p\mid c_i$, unde $0\leqslant i\leqslant n-1$. Vom demonstra că $p\mid c_{i+1}$. Într-adevăr,

$$f(x_{i+2})=c_{i+1}(x_{i+2}-x_1)\ldots(x_{i+2}-x_{i+1})+$$
$$+c_i(x_{i+2}-x_1)\ldots(x_{i+2}-x_i)+$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$+c_1(x_{i+2}-x_1)+$$
$$+c_0.$$

Deoarece $f(x_{i+2}) \equiv 0 \pmod p$ și $p|c_0,\ p|c_1, \ldots,\ p|c_i$ avem

$$c_{i+1}(x_{i+2}-x_1)\ldots(x_{i+2}-x_{i+1}) \equiv 0 \pmod p,$$

deci $p|c_{i+1}(x_{i+2}-x_1)\ldots(x_{i+2}-x_{i+1})$. Dar $x_{i+2} \not\equiv x_1 \pmod p, \ldots,$ $x_{i+2} \not\equiv x_{i+1} \pmod p$, deci $p \nmid x_{i+2}-x_1, \ldots, p \nmid x_{i+2}-x_{i+1}$, deci $p|c_{i+1}$. Am demonstrat, deci, prin inducție completă că:

$$p|c_0,\ p|c_1, \ldots,\ p|c_n.$$

Însă am arătat, în cadrul demonstrației teoremei precedente, că:

$$a_n = c_n,$$
$$a_{n-1} = c_{n-1} + b_{n-1,n}c_n,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$a_0 = c_0 + c_1 b_{0,1} + \ldots + c_{n-1}b_{0,n-1} + c_n b_{0,n},$$

deci $p|a_0,\ p|a_1, \ldots,\ p|a_{n-1},\ p|a_n$.

Capitolul 3

CLASE DE RESTURI

3.1. Clase de echivalență

Relația de congruență în inelul numerelor întregi este o *relație de echivalență*, deoarece are proprietățile de *reflexivitate*, *simetrie* și *tranzitivitate*.

Pentru a arăta că elementele a și b ale unei mulțimi se află într-o relație care este de echivalență vom scrie

$$a \sim b,$$

($\sim$ (tilda) trebuie citit „este echivalent cu"), iar proprietățile relației de echivalență le vom exprima astfel:

(a) *reflexivitate*: $a \sim a$,

(b) *simetrie*: $a \sim b \Rightarrow b \sim a$,

(c) *tranzitivitate*: $a \sim b \,\&\, b \sim c \Rightarrow a \sim c$.

De fiecare dată cînd între elementele unei mulțimi se stabilește o relație de echivalență, putem grupa elementele acestei mulțimi în clase de echivalență care se definesc în felul următor:

Definiție. *Clasă de echivalență este o submulțime a unei mulțimi între elementele căreia a fost stabilită o relație de echivalență, elementele submulțimii fiind toate elementele mulțimii considerate echivalente cu un element a al acestei mulțimi.*

Convenție. Clasa de echivalență definită mai sus se notează C_a

Definiție. *Elementul a de la care se pleacă pentru a alcătui clasa de echivalență C_a este reprezentantul clasei C_a.*

Clasele de echivalență au următoarele proprietăți :

(a) $b \in C_a \& c \in C_a \Rightarrow b \sim c$.

Într-adevăr, dacă $b \in C_a \& c \in C_a$ avem

$$b \sim a \& c \sim a.$$

Însă $c \sim a \Rightarrow a \sim c$ deci $b \sim a \& a \sim c \Rightarrow b \sim c$.

(b) $c \in C_a \& c \in C_b \Rightarrow C_a = C_b$.

Într-adevăr, dacă $d \in C_a$ din $d \in C_a \& c \in C_a$ rezultă $d \sim c$ conform proprietății (*a*) a claselor de echivalență. Din $c \in C_b$ rezultă $c \sim b$ deci din $d \sim c \& c \sim b$ rezultă $d \sim b$ deci $d \in C_b$, ceea ce înseamnă că $C_a \subset C_b$. Analog se arată că $C_b \subseteq C_a$ deci $C_a = C_b$.

(c) $C_a = C_b \Leftrightarrow a \sim b$.

Într-adevăr, din $C_a = C_b$ rezultă $a \in C_a$ deci $a \in C_b$, prin urmare $a \sim b$. Apoi din $a \sim b$ rezultă $a \in C_b$ și cum $a \in C_a$ obținem $C_a = C_b$ conform proprietății (*b*) a claselor de echivalență.

Observații

(1) Datorită proprietății (*c*) a claselor de echivalență, orice element al unei clase de echivalență poate fi luat drept *reprezentantul* acestei clase.

(2) Relația de egalitate în mulțimea claselor de echivalență ale unei mulțimi este o relație de echivalență. Aceasta se constată cu ajutorul proprietății (*c*) a claselor de echivalență.

(3) Împărțirea unei mulțimi în clase de echivalență constă în împărțirea mulțimii date în submulțimi astfel încît fiecare element al mulțimii să se afle într-o submulțime și numai în una singură. O astfel de împărțire a unei mulțimi în submulțimi se numește o *partiție* a mulțimii considerate.

Orice partiție a unei mulțimi generează o relație de echivalență în mulțimea considerată dacă fiind date elementele *a* și *b* ale mulțimii considerate se spune că aceste elemente sînt echivalente ($a \sim b$) numai dacă aparțin aceleiași submulțimi formate cu ajutorul partiției.

Într-adevăr, orice element *a* al mulțimii considerate aparține unei submulțimi și numai unei singure, deci $a \sim a$. Apoi două elemente *a*, *b* dacă aparțin unei submulțimi atunci elementele *b*, *a* aparțin și ele aceleiași submulțimi, deci $a \sim b \Rightarrow b \sim a$. În fine dacă *a*, *b* aparțin unei submulțimi, iar *b*, *c* aparțin aceleiași submulțimi, atunci *a*, *c* aparțin, de asemenea, aceleiași submulțimi, deci $a \sim b \& b \sim c \Rightarrow a \sim c$.

3.2. Clase de resturi modulo m

Relația de congruență în inelul numerelor întregi fiind o relație de echivalență, putem forma clase de echivalență pe care le vom numi *clase de resturi* sau *clase de resturi modulo m*, în care *m* este modulul relației de congruență în inelul numerelor întregi. Definiția claselor de echivalență în cazul claselor de resturi arată astfel.

Definiție. *Clasă de resturi este mulțimea tuturor numerelor întregi congruente modulo m cu un număr întreg dat.*

Convenție. Clasa de resturi o vom nota C_a ca orice clasă de echivalență, *a* fiind un număr întreg, reprezentantul clasei, dar vom mai folosi și notația $\hat{r}$, unde *r* este restul împărțirii lui *a* prin modulul *m*, în cazul în care $m \neq 0$. Numărul întreg $r \in C_a$, deoarece $a = mq + r$, $0 \leqslant r < |m|$ implică $m \mid a - r$, deci *r* poate fi luat drept reprezentant al clasei C_a, iar notația $\hat{r}$ este considerată ca având același sens ca notația C_r. În notația folosită pentru clase de resturi modulo *m* nu este nevoie să indicăm și modulul *m*, deoarece modulul este același pentru toate clasele de resturi formate cu ajutorul relației de congruență în inelul numerelor întregi.

Observație. În privința relației de egalitate în mulțimea claselor de resturi modulo *m*, reținem, conform celor spuse despre clasele de echivalență, că

$$C_a = C_b \Leftrightarrow a \equiv b \pmod{m}.$$

3.3. Inelul claselor de resturi modulo m

Mulțimea claselor de resturi modulo m o putem organiza ca un inel definind suma și produsul a două clase de resturi modulo m în felul următor.

Definiție. *Suma C_a+C_b a două clase de resturi C_a, C_b este clasa de resturi C_{a+b}, iar produsul C_aC_b, al acelorași clase de resturi, este clasa de resturi C_{ab}.*

Pentru a arăta că C_{a+b} este suma C_a+C_b, iar C_{ab} este produsul C_aC_b vom scrie

$$C_{a+b}=C_a+C_b,$$

$$C_{ab}=C_aC_b.$$

Observație. Suma și produsul astfel definite sînt unice, deoarece două relații de congruență în raport cu un același modul se adună și se înmulțesc membru cu membru. Din această cauză dacă $C_a=C_{a'}$, și $C_b=C_{b'}$, avem $C_{a+b}=C_{a'+b'}$, și $C_{ab}=C_{a'b'}$, deoarece din $a\equiv a' \pmod m$ și $b\equiv b' \pmod m$ deducem $a+b\equiv a'+b' \pmod m$ și $ab\equiv a'b' \pmod m$.

Exemplul 1. În cazul modulului $m=2$ avem două clase de resturi $\hat{0}$ și $\hat{1}$. În clasa $\hat{0}$ se află numai numere pare (divizibile cu 2), deoarece dacă $a\in\hat{0}$ atunci

$$a\equiv 0 \pmod 2,$$

deci $2|a-0$ sau $2|a$. Orice număr par se află în clasa $\hat{0}$, deoarece dacă $2|a$ avem $2|a-0$, deci $a\equiv 0 \pmod 2$ sau $a\in\hat{0}$. Deci clasa $\hat{1}$ este formată din toate numerele impare (nedivizibile cu 2).

Pentru modulul $m=2$ sumele și produsele claselor de resturi se dau cu ajutorul tablelor de adunare și de înmulțire care sînt tablouri cu două intrări și o ieșire și arată în felul următor:

Tabla de adunare

$+$	$\hat{0}$	$\hat{1}$
$\hat{0}$	$\hat{0}$	$\hat{1}$
$\hat{1}$	$\hat{1}$	$\hat{0}$

Tabla de înmulțire

$\times$	$\hat{0}$	$\hat{1}$
$\hat{0}$	$\hat{0}$	$\hat{0}$
$\hat{1}$	$\hat{0}$	$\hat{1}$

Exemplul 2. În cazul modulului $m=3$ avem trei clase de resturi $\hat{0}$, $\hat{1}$ și $\hat{2}$. Pentru modulul $m=3$ tablele de adunare și înmulțire pentru clasele de resturi sînt următoarele:

Tabla de adunare

	$\hat{0}$	$\hat{1}$	$\hat{2}$
$\hat{0}$	$\hat{0}$	$\hat{1}$	$\hat{2}$
$\hat{1}$	$\hat{1}$	$\hat{2}$	$\hat{0}$
$\hat{2}$	$\hat{2}$	$\hat{0}$	$\hat{1}$

Tabla de înmulțire

	$\hat{0}$	$\hat{1}$	$\hat{2}$
$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$
$\hat{1}$	$\hat{0}$	$\hat{1}$	$\hat{2}$
$\hat{2}$	$\hat{0}$	$\hat{2}$	$\hat{1}$

Mulțimea claselor de resturi modulo m înzestrată cu operațiile de adunare și înmulțire a claselor de resturi este un inel, deoarece:

(0) *Fiecărei perechi de clase de resturi C_a, C_b îi corespunde o singură clasă de resturi C_{a+b} numită sumă și o singură clasă de resturi C_{ab} numită produs.*

(I) *Adunarea are următoarele proprietăți:*

(a) *asocialivitate*: $(C_a+C_b)+C_c=C_a+(C_b+C_c)$,

(b) *comutalivitate*: $C_a+C_b=C_b+C_a$,

(c) *existența soluției C_{b-a} a ecuației $C_a+x=C_b$, oricare ar fi clasele de resturi C_a, C_b.*

(II) *Înmulțirea are proprietatea:*

(a) *asocialivitate*: $(C_aC_b)C_c=C_a(C_bC_c)$.

(III) *Înmulțirea este distributivă față de adunare:*

(a) $C_a(C_b+C_c)=C_aC_b+C_aC_c$,

(b) $(C_b+C_c)C_a=C_bC_a+C_cC_a$.

Inelul claselor de resturi modulo m este un inel comutativ cu element unitate, deoarece înmulțirea mai are următoarele proprietăți:

(b) *comutalivitate*: $C_aC_b=C_bC_a$,

(c1) *existența unui element, notat C_1, numit element neutru la înmulțire $C_aC_1=C_a$.*

Demonstrațiile acestor proprietăți se obțin utilizînd definițiile sumei și produsului claselor de resturi și constatînd că în ambii membri ai fiecărei egalități se capătă clase de resturi cu același reprezentant.

Observații.

(1) În definiția inelului (v. cap. 1) intră numai existența soluției ecuației $a+x=b$ oricare ar fi elementele a și b ale inelului. Unicitatea soluției acestei ecuații se demonstrează.

Unicitatea soluției ecuației $C_a+x=C_b$, în care C_a și C_b sînt clase de resturi se poate demonstra în două moduri.

Prima demonstrație folosește faptul că C_{b-a} este o soluție a ecuației $C_a+x=C_b$. Deci orice soluție C_c a ecuației $C_a+x=C_b$ satisface egalitatea $C_a+C_c=C_b$, deci $C_{a+c}=C_b$, de unde $a+c\equiv b \pmod m$, prin urmare $c\equiv b-a \pmod m$, așadar $C_c=C_{b-a}$.

A doua demonstrație se face prin reducere la absurd. Se presupune că două clase de resturi C_c, C_d, $C_c\neq C_d$, sînt soluții ale ecuației $C_a+x=C_b$. Atunci $C_a+C_c=C_b$, $C_a+C_d=C_b$ sau $C_{a+c}=C_b$, $C_{a+d}=C_b$ deci $C_{a+c}=C_{a+d}$. Prin urmare $a+c\equiv a+d \pmod m$. Reducîndu-l pe a obținem $c\equiv d \pmod m$, deci $C_c=C_d$, ceea ce vine în contradicție cu $C_c\neq C_d$. Prin urmare presupunerea făcută $C_c\neq C_d$ nu este adevărată și deci ecuația $C_a+x=C_b$ are soluție unică.

(2) Determinarea soluției C_{b-a} a ecuației $C_a+x=C_b$ se face cu ajutorul primei demonstrații a unicității soluției ecuației $C_a+x=C_b$. Deci demonstrînd unicitatea soluției ecuației $C_a+x=C_b$ utilizînd primul mod de demonstrație și presupunînd existența soluției ecuației considerate, putem demonstra și existența soluției acestei ecuații, avînd forma explicită a soluției, căpătată în urma demonstrației unicității soluției ecuației considerate.

(3) Proprietatea că ecuația $C_a+x=C_b$ are soluție unică, oricare ar fi clasele de resturi C_a, C_b definește diferența a două clase de resturi, anume

$$C_{b-a}=C_b-C_a$$

în definiția diferenței punîndu-se accentul atît pe existența cît și pe unicitatea ei.

(4) Ecuația $C_ax=C_b$ nu are soluții oricare ar fi clasele de resturi C_a, C_b.

Într-adevăr, ecuația $C_ax=C_b$ are soluții dacă și numai dacă congruența $ax\equiv b \pmod m$ are soluții, deoarece dacă $C_ax=C_b$ are soluții, notînd cu C_c soluția acestei ecuații, avem $C_aC_c=C_b \Leftrightarrow C_{ac}=C_b$, $C_{ac}=C_b \Leftrightarrow ac\equiv b \pmod m$ ceea ce înseamnă că congruența $ax\equiv b \pmod m$ are soluții. Dar congruența $ax\equiv b \pmod m$ are soluții dacă și numai dacă $d|b$, $d\cong(a, m)$. Deci

congruența $ax\equiv b \pmod m$ poate să nu aibă soluții dacă $d\nmid b$ sau poate avea soluții dacă $d|b$, dar soluția poate să nu fie unică în cazul cînd $d\neq 1$, $d>0$.

Dacă $d=1$ ecuația $ax\equiv b \pmod m$ are soluție unică, deoarece $d|b$, $d=1$, deci putem defini cîtul a două clase de resturi ca fiind clasa de resturi C_c soluție a ecuației $C_ax=C_b$:

$$C_c=C_b : C_a$$

în definiția cîtului punîndu-se accentul atît pe existența cîtului cît și pe unicitatea lui. Deci cîtul C_c a două clase de resturi C_b, C_a, numitorul fiind C_a, poate fi definit dacă și numai dacă $(a, m)=1$.

3.4. Clase de resturi prime cu modulul

Două numere întregi a și m pentru care $(a, m)\cong 1$ (al căror cel mai mare divizor comun este asociat cu 1) se numesc prime între ele sau se spune că a este prim cu m.

Definiție. *O clasă de resturi este primă cu modulul m dacă fiecare număr întreg din clasa de resturi considerată este prim cu modulul m.*

Teoremă. *Condiția necesară și suficientă ca o clasă de resturi să fie primă cu modulul este ca reprezentantul clasei de resturi considerate să fie prim cu modulul.*

Demonstrație. E suficient ca reprezentantul unei clase de resturi să fie prim cu modulul m ca clasa de resturi considerată să fie primă cu modulul, deoarece, conform proprietății care spune că dacă $a\equiv b \pmod m$ și $(a, m)\cong 1$ atunci $(b, m)\cong 1$, se constată că din $b\in C_a$ avem $b\equiv a \pmod m$ deci $a\equiv b \pmod m$ și dacă $(a, m)\cong 1$ atunci $(b, m)\cong 1$. E și necesar ca reprezentantul unei clase de resturi să fie prim cu modulul m ca clasa de resturi considerată să fie primă cu modulul, deoarece reprezentantul unei clase de resturi este unul dintre numerele întregi din clasa de resturi considerată.

Consecință. Există numai două tipuri de clase de resturi. Unele care sînt prime cu modulul și altele în care orice număr întreg conținut în ele este neprim cu modulul. Într-adevăr, nu este

posibil ca într-o clasă de resturi să avem un număr întreg a prim cu modulul și un număr întreg b neprim cu modulul, deoarece luîndu-l pe a ca reprezentantul clasei atunci și b trebuie să fie prim cu modulul, conform teoremei demonstrate mai sus.

3.5. Grupul multiplicativ al claselor de resturi prime cu modulul

Dacă se consideră numai mulțimea tuturor claselor de resturi prime cu modulul, atunci, față de operația de înmulțire a claselor de resturi, această mulțime formează un grup multiplicativ abelian), deoarece :

(0) *Fiecărei perechi* C_a, C_b *de clase de resturi prime cu modulul* m, *distincte sau nu, îi corespunde o clasă* C_{ab} *și numai una singură, primă cu modulul* m, *numită produsul celor două clase considerate.*

Demonstrație. Pentru a arăta existența produsului a două clase de resturi prime cu modulul m, nu este suficient să ne referim a faptul că C_{ab} este o clasă de resturi, ci mai trebuie să arătăm că această clasă de resturi este primă cu modulul m atunci cînd clasele de resturi C_a și C_b sînt prime cu modulul m. Trebuie să arătăm, deci, că

$$\text{dacă } (a,\ m)\cong 1 \text{ și } (b,\ m)\cong 1 \text{ atunci } (ab,\ m)\cong 1.$$

Aceasta se demonstrează scriind că

$$ra+sm=1 \text{ și } pb+qm=1,$$

unde r, s, p, q sînt numere întregi, deoarece condiția necesară și suficientă ca două numere întregi să fie prime între ele este ca să existe o combinație liniară de cele două numere cu coeficienți numere întregi egală cu 1. Dar

$$(ra+sm)(pb+qm)=1,$$

deci

$$(rp)(ab)+(rqa+spb+sqm)m=1$$

și cum rp și $rqa+spb+sqm$ sînt numere întregi înseamnă că ab și m sînt prime între ele, adică $(ab,\ m)\cong 1$. Cu aceasta existența produsului a două clase de resturi prime cu modulul este dovedită.

Unicitatea produsului a două clase de resturi prime cu modulul rezultă din unicitatea produsului a două clase de resturi.

(1) *Operația de înmulțire a claselor de resturi prime cu modulul este asociativă*, adică

$$(C_aC_b)C_c=C_a(C_bC_c).$$

Demonstrație. Aceasta rezultă din aceea că operația de înmulțire a claselor de resturi este asociativă.

(2) *Operația de înmulțire a claselor de resturi prime cu modulul este comutativă*, adică

$$C_aC_b=C_bC_a.$$

Demonstrație. Aceasta rezultă din aceea că operația de înmulțire a claselor de resturi este comutativă.

(3) *Ecuația* $C_ax=C_b$ *are soluții, oricare ar fi clasele de resturi* C_a, C_b *prime cu modulul* m.

Demonstrație. Existența soluției C_c, primă cu modulul m, a ecuației $C_ax=C_b$, în care C_a, C_b sînt clase de resturi prime cu modulul m rezultă în felul următor. Congruența $ax\equiv b \pmod m$ are soluții, deoarece $(a,\ m)\cong 1$. Fie c un număr întreg soluție a congruenței $ax\equiv b \pmod m$. Atunci $ac\equiv b \pmod m$ și cum $(b,\ m)\cong 1$ rezultă $(ac,\ m)\cong 1$ deci $(c,\ m)\cong 1$. Din $ac\equiv b \pmod m$ rezultă și $C_{ac}=C_b$, deci $C_aC_c=C_b$ și, prin urmare, C_c este o clasă de resturi primă cu modulul m, soluție a ecuației $C_ax=C_b$ în care C_a, C_b sînt clase de resturi prime cu modulul m.

Am utilizat proprietatea că

$$\text{dacă } (ac,\ m)\cong 1 \text{ atunci } (a,\ m)\cong 1 \text{ și } (c,\ m)\cong 1.$$

Aceasta este adevărat, deoarece dacă $(ac,\ m)\cong 1$, atunci există două numere întregi r și s astfel încît

$$r(ac)+sm=1.$$

Dar atunci $(rc)a+sm=1$, unde rc și s sînt numere întregi, deci $(a,\ m)\cong 1$ și $(ra)c+sm=1$, unde ra și s sînt numere întregi, deci $(c,\ m)\cong 1$.

Observație. Soluția ecuației $C_ax=C_b$, în care C_a, C_b sînt clase de resturi prime cu modulul m, este unică, deoarece orice soluție C_c a acestei ecuații conduce la o soluție c a congruenței $ax\equiv b \pmod m$, iar soluția acestei congruențe este unică avînd $d=1$, $d\cong(a,\ m)$, $d>0$.

3.6. Corpul claselor de resturi față de un modul prim

Un corp este un inel cu următoarele proprietăți suplimentare:
(a) *Conține cel puțin un element diferit de elementul* 0;
(b) *ecuațiile*

$$ax=b,$$
$$ya=b$$

au soluții oricare ar fi a *și* b, $a\neq 0$.

În inelul claselor de resturi rolul elementului 0 îl joacă clasa de resturi C_0.

Teoremă. *Inelul claselor de resturi este corp dacă și numai dacă modulul este prim.*

Demonstrație. Dacă modulul m este prim, atunci, cu excepția lui 0, toate numerele r pentru care $0\leqslant r<|m|$ sînt prime cu m. Într-adevăr, dacă $0\leqslant r<|m|$, $r\neq 0$, iar m este prim, trebuie să avem $(r, m)\cong 1$, deoarece dacă $m|r$ atunci $|m|\leqslant|r|$, pentru că $r\neq 0$, ceea ce este contradictoriu. În această demonstrație ne-am bazat pe aceea că numerele prime p au proprietatea că pentru fiecare număr întreg a avem

$$p|a \text{ sau } (a, p)\cong 1$$

„sau" fiind cu excludere. Această proprietate are loc, deoarece luînd $(a, p)\cong d$ avem $d|p$. Numărul p fiind prim putem avea numai $d=\pm p$ sau $d=\pm 1$, „sau" fiind cu excludere, deoarece $p\neq\pm 1$, fiind prim. Dacă $d=\pm p$, deoarece $d|a$ avem $p|a$. Dacă $d=\pm 1$ avem $(a, p)\cong 1$.

Deci în cazul cînd modulul m este prim, rezultă că toate clasele de resturi $\hat{r}$ cu excepția lui $\hat{0}$ sînt prime cu modulul. Atunci ecuațiile

$$C_a x=C_b,$$
$$yC_a=C_b$$

au soluții oricare ar fi clasele C_a și C_b, $C_a\neq C_0$.

Inelul claselor de resturi față de un modul prim m conține clasa C_1, $C_1\neq C_0$, deoarece m fiind prim este diferit de ± 1, deci $1\not\equiv 0 \pmod m$.

Așadar inelul claselor de resturi cînd modulul este prim se transformă într-un corp.

Pentru a arăta că inelul claselor de resturi este corp numai dacă modulul este prim, vom considera că modulul m nu este prim. Atunci m este compus sau o unitate în inelul numerelor întregi. În cazul cînd m este compus putem avea $m=0$ sau $m\neq 0$.

Dacă $m=0$, ecuația

$$C_a x=C_0$$

admite soluții numai dacă ecuația $ax=b$ admite soluții. Dacă $C_a\neq C_0$, atunci $a\neq 0$. Dar există numere întregi a și b, $a\neq 0$, astfel ca $a\nmid b$ și atunci ecuația $ax=b$ nu admite soluții deși $a\neq 0$. Pentru acest motiv inelul claselor de resturi modulo 0 nu este corp.

Dacă m este compus și diferit de zero, există un divizor propriu n al lui m. Aceasta înseamnă că $n|m$, $n\neq\pm 1$, $n\neq\pm m$. Dar atunci ecuația

$$C_a x=C_b,$$

în care $C_a=C_n$ nu admite soluții dacă $n\nmid b$ deși $C_a\neq C_0$. Într-adevăr, ecuația $C_a x=C_b$ are soluții numai dacă congruența $ax\equiv b \pmod m$ are soluții, iar congruența $ax\equiv b \pmod m$ are soluții numai dacă $d|b$, unde $d\cong(a, m)\cong(n, m)\cong n$. Avem $C_a\neq C_0$, deoarece dacă am presupune prin absurd că $C_a=C_0$, atunci am avea $C_n=C_0$ sau $n\equiv 0 \pmod m$, deci $m|n-0$, adică $m|n$ și cum mai avem $n|m$ am obține $n=\pm m$, ceea ce este contradictoriu, n fiind divizor propriu al lui m.

Dacă m este o unitate în inelul numerelor întregi, adică $m=\pm 1$, mulțimea claselor de resturi modulo m are un singur element C_0 și deci nici nu se pune problema ca această mulțime să fie corp, deoarece în această mulțime nu există clase de resturi diferite de clasa C_0.

Deci dacă modulul m nu este prim, inelul claselor de resturi modulo m nu este corp.

3.7. Relația de congruență în inelul numerelor m-întregi

Definiție. *Un număr rațional este* m*-întreg dacă poate fi scris sub forma* $\frac{a}{b}$, *unde* a *și* b *sînt numere întregi, iar* $(b, m)\cong 1$, m *fiind un număr întreg.*

Observație. Orice număr întreg a este în același timp m-întreg, deoarece putem scrie $a=\frac{a}{1}$, iar $(1, m)\cong 1$. Deci mulțimea numerelor întregi este inclusă în mulțimea numerelor m-întregi.

Mulțimea numerelor m-întregi o putem organiza ca un inel definind suma și produsul a două numere m-întregi în felul următor.

Definiție. *Suma a două numere α și β m-întregi este numărul rațional $\alpha+\beta$, iar produsul acelorași numere m-întregi este numărul rațional $\alpha\beta$.*

Observație. Suma și produsul a două numere m-întregi există, deoarece dacă $\alpha=\frac{a}{b}$, $\beta=\frac{c}{d}$, unde a, b, c, d sînt numere întregi, iar $(b, m)\cong 1$, $(d, m)\cong 1$, atunci $\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$, $\frac{a}{b}\frac{c}{d}=\frac{ac}{bd}$, unde $ad+bc$, bd, ac, bd sînt numere întregi, iar $(bd,m)\cong 1$.

Unicitatea sumei și a produsului a două numere m-întregi rezultă din unicitatea sumei și produsului a două numere raționale.

Teoremă. *Mulțimea numerelor m-întregi formează un inel comutativ cu element unitate față de adunarea și înmulțirea numerelor m-întregi.*

Demonstrație.

(0) Fiecărei perechi α, β de numere m-întregi îi corespunde un singur număr $\alpha+\beta$ m-întreg numit sumă și un singur număr $\alpha\beta$ m-întreg numit produs.

(I) Adunarea are următoarele proprietăți:

(a) asociativitate: $(\alpha+\beta)+\gamma=\alpha+(\beta+\gamma)$,

(b) comutativitate: $\alpha+\beta=\beta+\alpha$,

(c) existența soluției ecuației $\alpha=\beta+x$, oricare ar fi numerele α și β m-întregi.

(II) Înmulțirea are următoarele proprietăți:

(a) asociativitate: $(\alpha\beta)\gamma=\alpha(\beta\gamma)$,

(b) comutativitate: $\alpha\beta=\beta\alpha$,

(c1) existența unui element, notat 1, numit element neutru la înmulțire $\alpha\cdot 1=\alpha$.

(III) Înmulțirea este distribuită față de adunare:

(a) $\alpha(\beta+\gamma)=\alpha\beta+\alpha\gamma$.

Toate aceste proprietăți ale numerelor m-întregi sînt adevărate, deoarece ele sînt adevărate pentru numere raționale, existența soluției ecuației $\alpha=\beta+x$, oricare ar fi numerele α și β m-întregi, rezultînd din aceea că soluția este $\alpha+(-\beta)$, $-\beta$ fiind opusul numărului rațional β, iar $-\beta$ este m-întreg îndată ce β este m-întreg.

Observație. Dacă $m=\pm 1$ inelul numerelor m-întregi devine corpul numerelor raționale.

Dacă însă $m\neq\pm 1$ inelul numerelor m-întregi nu este corp. Într-adevăr, să considerăm ecuația $ax=b$, unde a, b sînt numere întregi prime între ele, $a\neq 0$, $(a, m)\ncong 1$. În corpul numerelor raționale soluția ecuației $ax=b$ este $\frac{b}{a}$ care nu este m-întreg, deoarece dacă prin absurd $\frac{b}{a}$ ar fi m-întreg, ar exista un număr rațional $\frac{c}{d}$ cu $(d, m)\cong 1$ astfel încît $\frac{b}{a}=\frac{c}{d}$. Dar a, b fiind prime între ele, fracția $\frac{b}{a}$ este ireductibilă, deci există un număr întreg t astfel încît $c=tb$, $d=ta$ și cum $(d, m)\cong 1$ ar însemna ca $(a, m)\cong 1$, ceea ce contrazice $(a, m)\ncong 1$. Numărul rațional $\frac{b}{a}$ nefiind m-întreg înseamnă că ecuația $ax=b$ nu are soluții în inelul numerelor m-întregi și deci acest inel nu poate fi corp.

3.7.1. Relația de divizibilitate în inelul numerelor m-întregi

Definiție. *Un număr m-întreg α se divide cu un număr m-întreg β dacă există un număr m-întreg γ astfel încît*

$$\alpha=\beta\gamma.$$

Pentru a arăta că β divide pe α se scrie $\beta\mid\alpha$.

Observație. Relația de divizibilitate în inelul numerelor m-întregi are proprietățile relației de divizibilitate în inelul numerelor întregi, deoarece demonstrațiile se bazează pe proprietățile

operațiilor de adunare și de înmulțire într-un inel, fie el inelul numerelor întregi, fie el inelul numerelor m-întregi. Trebuie doar ca noțiunile din inelul numerelor întregi să le înlocuim cu noțiunile corespunzătoare din inelul numerelor m-întregi. Astfel unitățile din inelul numerelor întregi care sînt 1 și -1 trebuie înlocuite cu unitățile din inelul numerelor m-întregi care sînt toate numerele raționale care pot fi scrise sub forma $\frac{a}{b}$, unde a și b sînt numere întregi, iar $(a, m)\cong 1$, $(b, m)\cong 1$. Într-adevăr, asemenea numere m-întregi divid pe 1, deoarece $1=\frac{a}{b}\frac{b}{a}$, $\frac{b}{a}$ fiind m-întreg, datorită lui $(a, m)\cong 1$. Numai asemenea numere m-întregi divid pe 1, deoarece ecuația $1=\alpha x$ cu $\alpha\neq 0$ m-întreg nu admite soluții dacă $\alpha=\frac{c}{d}$, $(c, m)\ncong 1$. Într-adevăr, în fracția ireductibilă $\frac{a}{b}$ a lui $\frac{c}{d}$ avem $(a, m)\ncong 1$, deoarece din $\frac{c}{d}=\frac{a}{b}$ rezultă că există un număr întreg t astfel încît $c=at$, $d=bt$ și cum din $(d, m)\cong 1$ rezultă $(t, m)\cong 1$, înseamnă că $(a, m)\ncong 1$, pentru că, în caz contrar, am avea $(c, m)\cong 1$. Însă mai sus am văzut că ecuația $ax=b$ cu a și b numere întregi prime între ele, $a\neq 0$, $(a, m)\ncong 1$ nu admite ca soluție un număr m-întreg, deci nici ecuația $\frac{a}{b}x=1$ sau $1=\alpha x$ nu admite ca soluție un număr m-întreg.

3.7.2. Relația de congruență în inelul numerelor m-întregi

Definiție. *Două numere m-întregi α și β sînt congruente modulo m, unde m este un număr întreg, dacă $m|\alpha-\beta$.*

Pentru a arăta că $m|\alpha-\beta$ se scrie

$$\alpha\equiv\beta \pmod m.$$

Observație. Relația de congruență în inelul numerelor m-întregi are toate proprietățile relației de congruență în inelul numerelor întregi care rezultă din proprietățile relației de divizibilitate în inelul numerelor întregi, deoarece relația de divizibilitate în inelul numerelor m-întregi are toate proprietățile relației de divizibilitate în inelul numerelor întregi, după cum am văzut mai sus.

Teoremă. *Dacă numerele m-întregi α și β se prezintă sub forma $\frac{a}{b}$, $\frac{c}{d}$, unde a, b, c, d sînt numere întregi, $(b, m)\cong 1$, $(d, m)\cong 1$, atunci congruența*

$$\alpha\equiv\beta \pmod m$$

definită în inelul numerelor m-întregi este echivalentă cu congruența

$$ad\equiv bc \pmod m$$

definită în inelul numerelor întregi.

Demonstrație. Congruența $\alpha\equiv\beta \pmod m$ fiind definită în inelul numerelor m-întregi înseamnă că $m|\alpha-\beta$ în inelul numerelor m-întregi, deci există un număr m-întreg γ astfel încît $\alpha-\beta=m\gamma$. Deci putem scrie $\gamma=\frac{g}{h}$, unde g și h sînt numere întregi, iar $(h, m)\cong 1$. Atunci din $\alpha-\beta=m\gamma$ obținem $(ad-bc)h=mgbd$. Deci $m|(ad-bc)h$ în inelul numerelor întregi și cum $(h, m)\cong 1$ rezultă $m|ad-bc$ în inelul numerelor întregi sau $ad\equiv bc \pmod m$ în inelul numerelor întregi. Reciproc, din congruența $ad\equiv bc \pmod m$, definită în inelul numerelor întregi, obținem $m|ad-bc$ în inelul numerelor întregi, deci există un număr întreg g astfel încît $ad-bc=mg$. Prin urmare $\frac{a}{b}-\frac{c}{d}=m\frac{g}{bd}$, unde $\frac{g}{bd}$ este un număr m-întreg g și bd fiind numere întregi iar $(bd, m)\cong 1$. Așadar $m|\alpha-\beta$ în inelul numerelor m-întregi deci congruența $\alpha\equiv\beta \pmod m$ este definită în inelul numerelor m-întregi.

Observație. Proprietatea pe care am demonstrat-o ne arată că congruența $a\equiv b \pmod m$, în care a și b sînt numere întregi definită în inelul numerelor întregi este definită și în inelul numerelor m-întregi și reciproc. Într-adevăr, congruența $a\equiv b \pmod m$ definită în inelul numerelor întregi, scrisă sub forma $a\cdot 1\equiv b\cdot 1 \pmod m$ este echivalentă cu congruența $\frac{a}{1}\equiv\frac{b}{1} \pmod m$, adică cu $a\equiv b \pmod m$ definită în inelul numerelor m-întregi.

3.7.3. Clase de resturi modulo m în inelul numerelor m-întregi

Putem face împărțirea în clase de resturi modulo m a numerelor m-întregi. Această împărțire în clase de resturi modulo m se reduce la îmbogățirea cu numere m-întregi a claselor de resturi modulo m formate din numere întregi. Aceasta se dovedește prin faptul că relația de congruență definită în inelul numerelor întregi este definită și în inelul numerelor m-întregi, care include inelul numerelor întregi, ținînd seama și de următoarea :

Teoremă. *Orice număr m-întreg este congruent modulo m în inelul numerelor m-întregi cu un număr întreg.*

Demonstrație. Dacă α este un număr m-întreg, îl putem scrie sub forma $\frac{a}{b}$, unde $(b, m) \cong 1$. Apoi congruența $\frac{a}{b} \equiv c \pmod m$ în inelul numerelor m-întregi, unde c este un număr întreg, este echivalentă cu congruența $a \equiv bc \pmod m$ în inelul numerelor întregi, iar congruența $a \equiv bx \pmod m$ admite soluții în inelul numerelor întregi în cazul cînd $(b, m) \cong 1$, deci există un număr întreg c astfel încît $a \equiv bc \pmod m$ în inelul numerelor întregi sau $\frac{a}{b} \equiv c \pmod m$ în inelul numerelor m-întregi.

Observație. Scriind numerele m-întregi sub forma ab^{-1}, unde $(b, m) \cong 1$, a și b fiind numere întregi și utilizînd relația de congruență în inelul numerelor m-întregi, putem scrie puteri negative ale numerelor întregi prime cu modulul m în oricare din cei doi membri ai unei congruențe.

Capitolul 4

TEOREMELE LUI EULER, FERMAT ȘI WILSON

4.1. Sisteme complete de resturi modulo m

Definiție. *Sistem complet de resturi modulo m este o mulțime de numere întregi formată din reprezentanții tuturor claselor de resturi modulo m din fiecare clasă de resturi fiind luat cîte un singur reprezentant.*

Teoremă. *Dacă m este un număr întreg diferit de zero, atunci numărul elementelor dintr-un sistem complet de resturi modulo m este egal cu $|m|$.*

Demonstrație. Putem lua ca reprezentanți ai claselor de resturi modulo m numerele întregi r diferite două cîte două, care au proprietatea că $0 \leqslant r < |m|$, conform celei de-a doua definiții a relației de congruență în inelul numerelor întregi, iar numărul acestor numere întregi este $|m|$.

Consecință. Dacă modulul m este un număr întreg diferit de zero, atunci numărul claselor de resturi diferite două cîte două este $|m|$.

Din contra, dacă $m=0$, atunci în fiecare clasă de resturi se află numai un număr întreg, relația de congruență reducîndu-se în acest caz la relația de egalitate, deci pentru $m=0$ există o infinitate de clase de resturi modulo 0.

Observație. Un sistem complet de resturi modulo m, în cazul cînd $m \neq 0$, este caracterizat prin următoarele două proprietăți:

(1) este format din $|m|$ numere întregi;

(2) diferența a două numere întregi oarecare din acest sistem nu se divide prin numărul întreg m.

Pentru a arăta că un sistem complet de resturi modulo m, în cazul cînd $m \neq 0$, este caracterizat prin cele două proprietăți de mai sus, trebuie să arătăm că orice sistem complet de resturi modulo m, în cazul cînd $m \neq 0$, are cele două proprietăți și că orice mulțime de numere întregi care are cele două proprietăți este un sistem complet de resturi modulo m. Vom arăta acest lucru.

Fiind dat un sistem complet de resturi modulo m, unde $m \neq 0$, în acest sistem avem $|m|$ elemente conform teoremei de mai sus, iar două elemente oarecare din acest sistem reprezentînd clase de resturi distincte sînt necongruente între ele, deci diferența lor nu este divizibilă cu m.

Reciproc, dacă pentru $m \neq 0$, luăm o mulțime de $|m|$ numere întregi, două numere oarecare din această mulțime neavînd diferența lor divizibilă cu m, înseamnă că fiecare număr din mulțimea considerată reprezintă cîte o clasă de resturi modulo m distinctă de clasele de resturi modulo m reprezentate de celelalte numere din mulțimea considerată. Deoarece conform consecinței, pentru $m \neq 0$, numărul claselor de resturi modulo m este egal cu $|m|$ înseamnă că fiecare clasă este reprezentată de un număr din mulțimea considerată, care în felul acesta este un sistem complet de resturi modulo m.

Teoremă. *Dacă* $c_1, c_2, \ldots, c_{|m|}$ *este un sistem complet de resturi modulo* m, m *fiind un număr întreg diferit de zero, iar* a *și* b *sînt numere întregi,* a *fiind prim cu* m, *atunci* $ac_1+b, ac_2+b, \ldots, ac_{|m|}+b$ *este, de asemenea, un sistem complet de resturi modulo* m.

Demonstrație. În $ac_1+b, ac_2+b, \ldots, ac_{|m|}+b$ avem $|m|$ numere întregi, iar dacă facem diferența $(ac_j+b)-(ac_i+b)=a(c_j-c_i)$, unde i și j sînt numere naturale luate din $1, 2, \ldots, |m|$, iar $j \neq i$, constatăm că $m \nmid a(c_j-c_i)$, deoarece dacă $m \mid a(c_j-c_i)$, ținînd seama de $(a, m)\cong 1$, avem și $m \mid c_j-c_i$, ceea ce nu se poate, deoarece c_i și c_j, unde $i \neq j$, iar $1 \leqslant i \leqslant |m|$, $1 \leqslant j \leqslant |m|$, reprezintă clase distincte de resturi modulo m, adică $c_i \not\equiv c_j \pmod m$. Deci pentru $ac_1+b, ac_2+b, \ldots, ac_{|m|}+b$ se verifică cele două proprietăți ale sistemelor complete de resturi modulo m, atunci cînd $m \neq 0$, anume că un sistem complet de resturi modulo m

(1) este format din $|m|$ numere întregi;

(2) diferența a două numere întregi oarecare din acest sistem nu se divide prin numărul întreg m.

Definiție. *Mai multe numere întregi sînt consecutive dacă ele sînt diferite două cîte două și printre ele găsim toate numerele întregi, dar numai aceste numere întregi, cuprinse între două numere întregi* a *și* b *diferite și neconsecutive.*

Teoremă. *Dacă* m *este un număr întreg diferit de zero, atunci* $|m|$ *numere întregi consecutive formează un sistem complet de resturi modulo* m.

Demonstrație. Fie $a+1, a+2, \ldots, a+|m|$ cele $|m|$ numere întregi consecutive. Aici avem $|m|$ numere întregi, iar dacă facem diferența $(a+j)-(a+i)=j-i$, unde i și j sînt numere naturale luate din $1, 2, \ldots, |m|$, iar $j \neq i$, constatăm că $m \nmid j-i$, deoarece dacă $m \mid j-i$ avem $|m| \leqslant |j-i|$, ceea ce nu se poate, pentru că $|j-i| \leqslant |m|-1$ sau $|j-i| < |m|$, ceea ce este contradictoriu. Deci mulțimea celor $|m|$ numere întregi consecutive, avînd cele două proprietăți care caracterizează un sistem complet de resturi modulo m, $m \neq 0$, este un sistem complet de resturi modulo m.

Consecință. Dacă m este un număr întreg diferit de zero, atunci din $|m|$ numere întregi consecutive unul din aceste numere întregi se divide cu m.

Într-adevăr, din cauză că cele $|m|$ numere întregi consecutive formează un sistem complet de resturi modulo m, înseamnă că unul din ei reprezintă clasa de resturi C_0, deci acest număr întreg se divide cu m, deoarece orice număr întreg din clasa de resturi C_0 este congruent cu 0 modulo m, deci se divide cu m.

4.2. Sisteme reduse de resturi modulo m

Definiție. *Sistem redus de resturi modulo* m *este o mulțime de numere întregi formată din reprezentanții tuturor claselor de resturi modulo* m, *prime cu modulul, din fiecare clasă de resturi primă cu modulul* m *fiind luat cîte un singur reprezentant.*

Teoremă. *Numerele întregi prime cu modulul* m *dintr-un sistem complet de resturi modulo* m *formează un sistem redus de resturi modulo* m.

Demonstrație. Fiecare număr întreg dintr-un sistem complet de resturi modulo m face parte dintr-o clasă de resturi modulo m și numai din una singură, deci, dacă reținem numerele întregi prime cu modulul m dintr-un sistem complet de resturi modulo m, obținem un sistem redus de resturi modulo m.

Teoremă. *Pentru fiecare număr întreg m, orice sistem redus de resturi modulo m este o mulțime finită.*

Demonstrație. Fiecare sistem redus de resturi modulo m poate fi conceput ca fiind o submulțime a unui sistem complet de resturi modulo m obținut din sistemul redus de resturi modulo m prin completarea acestuia cu reprezentanții claselor de resturi neprime cu modulul m. Dar pentru $m \neq 0$ orice sistem complet de resturi modulo m este o mulțime finită, avînd $|m|$ elemente, deci pentru $m \neq 0$ orice sistem redus de resturi modulo m este o mulțime finită fiind o submulțime a unei mulțimi finite care este un sistem complet de resturi modulo m obținut prin completarea în modul indicat mai de sus a sistemului redus de resturi modulo m considerat.

Dacă $m=0$, numerele întregi a care sînt prime cu modulul $m=0$ verifică relația $(a, 0) \cong 1$, de unde rezultă că $a \cong 1$, deoarece $(a, 0) \cong a$, iar cel mai mare divizor comun a două numere întregi are proprietatea de unicitate. Deci pentru $m=0$, fiecare clasă de resturi fiind formată din cîte un singur număr întreg, avem un singur sistem redus de resturi modulo 0 format din -1 și 1, care este deci o mulțime finită.

Observație. Numărul de elemente dintr-un sistem redus de resturi modulo m nu diferă de la un sistem redus de resturi modulo m la altul, deoarece acest număr este egal cu numărul claselor de resturi prime cu modulul m. Acest număr se notează cu $\varphi(m)$ și se numește indicatorul lui Euler al numărului întreg m. Putem vorbi de numărul de elemente dintr-un sistem redus de resturi modulo m, deoarece sistemele reduse de resturi modulo m sînt mulțimi finite.

Observație. Cu notația $\varphi(m)$ pentru numărul elementelor dintr-un sistem redus de resturi modulo m, putem caracteriza un sistem redus de resturi modulo m prin următoarele trei proprietăți:

(1) este format din $\varphi(m)$ numere întregi;

(2) diferența a două numere întregi oarecare din acest sistem nu se divide prin numărul întreg m;

(3) fiecare număr întreg din acest sistem este prim cu modulul m.

Pentru a arăta că un sistem redus de resturi modulo m este caracterizat prin cele trei proprietăți de mai sus, trebuie să arătăm că orice sistem redus de resturi modulo m are cele trei proprietăți și că orice mulțime de numere întregi care are cele trei proprietăți este un sistem redus de resturi modulo m. Vom arăta aceasta.

Fiind dat un sistem redus de resturi modulo m, în acest sistem avem $\varphi(m)$ numere întregi, două numere întregi oarecare din acest sistem, reprezentînd clase de resturi distincte, sînt necongruente între ele, deci diferența lor nu este divizibilă cu m, iar clasele de resturi reprezentate de numerele întregi din acest sistem fiind prime cu modulul m, înseamnă că și fiecare număr întreg dintr-un sistem redus de resturi modulo m este prim cu modulul.

Reciproc, dacă o mulțime de numere întregi are $\varphi(m)$ elemente, diferența a două numere întregi oarecare din această mulțime nefiind divizibilă cu m și fiecare din numerele întregi din mulțimea considerată este prim cu modulul, atunci mulțimea considerată este un sistem redus de resturi modulo m. Într-adevăr, numerele întregi din mulțimea considerată fiind prime cu modulul, înseamnă că ele reprezintă numai clase de resturi prime cu modulul. Fiecare clasă de resturi primă cu modulul este reprezentată, dar numai o dată, deoarece numărul claselor de resturi prime cu modulul m este $\varphi(m)$ și numărul numerelor întregi din mulțimea considerată este $\varphi(m)$ și dacă o clasă nu ar fi reprezentată, o altă clasă ar fi reprezentată de două ori, acest lucru întîmplîndu-se și atunci cînd o clasă nu ar fi reprezentată numai o dată. Dar atunci numerele întregi care ar reprezenta aceeași clasă ar fi congruente modulo m, deci diferența dintre ele s-ar divide cu m, ceea ce este contradictoriu.

Teoremă. *Dacă $c_1, c_2, \ldots, c_{\varphi(m)}$ este un sistem redus de resturi modulo m, iar a este un număr întreg prim cu m, atunci $ac_1, ac_2, \ldots, ac_{\varphi(m)}$ este, de asemenea, un sistem redus de resturi modulo m.*

Demonstrație. În $ac_1, ac_2, \ldots, ac_{\varphi(m)}$ avem $\varphi(m)$ numere întregi, iar dacă facem diferența $ac_j - ac_i = a(c_j - c_i)$, unde i și j sînt numere naturale luate din $1, 2, \ldots, \varphi(m)$, iar $j \neq i$, constatăm că $m \nmid a(c_j - c_i)$, deoarece dacă $m \mid a(c_j - c_i)$, avînd $(a, m) \cong 1$ avem și $m \mid c_j - c_i$, ceea ce nu se poate, deoarece c_i și c_j, unde

$i \neq j$, iar $1 \leqslant i \leqslant \varphi(m)$, $1 \leqslant j \leqslant \varphi(m)$, reprezintă clase distincte de resturi modulo m prime cu modulul, adică $c_i \not\equiv c_j \pmod m$. În plus, fiecare produs ac_i, unde $1 \leqslant i \leqslant \varphi(m)$, este prim cu modulul m, fiindcă atît a cît şi c_i, unde $1 \leqslant i \leqslant \varphi(m)$, sînt numere întregi prime cu m. Deci mulţimea de numere întregi $ac_1, ac_2, \ldots, ac_{\varphi(m)}$, avînd cele trei proprietăţi care caracterizează un sistem redus de resturi modulo m, este un sistem redus de resturi modulo m.

4.3. Indicatorul lui Euler

Definiţie. *Indicatorul lui Euler al unui număr întreg m este un număr natural egal cu numărul elementelor dintr-un sistem redus de resturi modulo m.*

Observaţie. În definiţie referirea se face la unul dintre sistemele reduse de resturi modulo m, deoarece numărul de elemente dintr-un sistem redus de resturi modulo m, oricare ar fi acest sistem, este egal cu numărul claselor de resturi prime cu modulul m. În această definiţie putem vorbi de numărul elementelor dintr-un sistem redus de resturi modulo m, deoarece sistemele reduse de resturi modulo m sînt mulţimi finite.

Convenţie. Indicatorul lui Euler al numărului întreg m se notează cu $\varphi(m)$.

Exemplul 1. Pentru $m=-7$ un sistem redus de resturi modulo -7 este mulţimea de numere întregi

$$1, 2, 3, 4, 5, 6,$$

deoarece 0, 1, 2, 3, 4, 5, 6 este un sistem complet de resturi modulo -7, iar numai 1, 2, 3, 4, 5, 6 sînt numere prime cu modulul -7. Numărul elementelor 1, 2, 3, 4, 5, 6 fiind 6, avem $\varphi(-7)=6$.

Exemplul 2. Pentru $m=14$ un sistem redus de resturi modulo 14 este mulţimea de numere întregi

$$1, 3, 5, 9, 11, 13,$$

deoarece 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13 este un sistem complet de resturi modulo 14, iar numai 1, 3, 5, 9, 11, 13 sînt prime cu modulul 14. Deci $\varphi(14)=6$.

Exemplul 3. Pentru $m=\pm 1$ un sistem redus de resturi modulo ± 1 este mulţimea formată din 0, deoarece 0 constituie un sistem complet de resturi modulo ± 1 şi 0 este prim cu ± 1. Deci $\varphi(1)=\varphi(-1)=1$.

Exemplul 4. Pentru $m=0$ un sistem redus de resturi modulo 0 este mulţimea formată din

$$-1, 1,$$

deoarece mulţimea numerelor întregi constituie un sistem complet de resturi modulo 0, iar numai -1 şi 1 sînt prime cu modulul 0. Deci $\varphi(0)=2$.

Observaţie. Indicatorul lui Euler al unui număr întreg m, $m \neq 0$, $m \neq \pm 1$ poate fi calculat atunci cînd se cunoaşte descompunerea lui m în factori primi. Formula de calcul a indicatorului lui Euler al unui număr întreg m pentru care $m \neq 0$, $m \neq \pm 1$ va rezulta din următoarele teoreme.

Teoremă. *Indicatorul lui Euler este o funcţie multiplicativă*, adică

$$\varphi(m)=\varphi(m_1)\varphi(m_2),$$

dacă $m=m_1m_2$ *şi* $(m_1, m_2) \cong 1$.

Demonstraţie. Dacă $m \neq 0$, vom considera următorul sistem complet de resturi modulo m

$$1, 2, 3, \ldots, |m|-2, |m|-1, |m|.$$

Numerele întregi prime cu modulul m care se află în acest sistem formează un sistem redus de resturi modulo m şi sînt deci în număr de $\varphi(m)$.

Dacă sistemul complet de resturi modulo m de mai sus îl vom scrie sub forma

$$\begin{array}{ccccc} 1 & & 2\ldots & & |m_1| \\ |m_1|+1 & & |m_1|+2\ldots & & |m_1|+|m_1| \\ 2|m_1|+1 & & 2|m_1|+2\ldots & & 2|m_1|+|m_1| \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ (|m_2|-1)|m_1|+1 & & (|m_2|-1)|m_1|+2\ldots & & (|m_2|-1)|m_1|+|m_1| \end{array}$$

vom constata următoarele.

Numerele întregi situate în aceeaşi coloană fac parte din aceeaşi clasă de resturi modulo m_1, deoarece diferenţa a două oarecare din ele se divide cu m_1.

Deci numerele întregi situate în aceeași coloană sau sînt toate prime cu m_1 sau sînt toate neprime cu m_1. Atunci cînd aceste numere întregi sînt neprime cu m_1, ele sînt neprime și cu m, deoarece $m=m_1m_2$.

Deci în coloanele în al căror vîrf se află un număr întreg neprim cu m_1 nu vom găsi nici un număr întreg prim cu m. Toate numerele întregi prime cu m din tabloul de mai sus se vor găsi deci în coloanele în al căror vîrf se află un număr întreg prim cu m_1.

Dar, în prima linie din tabloul de mai sus este scris un sistem complet de resturi modulo m_1, avînd $|m_1|$ numere întregi consecutive. Deci numărul coloanelor în care se găsesc toate numerele întregi prime cu m din tabloul de mai sus este egal cu numărul numerelor prime cu m_1 scrise în prima linie în tabloul de mai sus, care constituie deci un sistem redus de resturi modulo m_1 și al căror număr este deci $\varphi(m_1)$. Dacă notăm cu c_1, $c_2, \ldots, c_{\varphi(m_1)}$ sistemul redus de resturi modulo m_1 extras din sistemul $1, 2, \ldots, |m_1|$ complet de resturi modulo m_1, atunci, conform celor spuse mai sus, toate numerele prime cu m din tabloul de mai sus se află în tabloul de mai jos

$$\begin{array}{rrr}
c_1 & c_2 \ldots & c_{\varphi(m_1)} \\
|m_1|+c_1 & |m_1|+c_2 \ldots & |m_1|+c_{\varphi(m_1)} \\
2|m_1|+c_1 & 2|m_1|+c_2 \ldots & 2|m_1|+c_{\varphi(m_1)} \\
\ldots & \ldots & \ldots \\
(|m_2|-1)|m_1|+c_1 & (|m_2|-1)|m_1|+c_2 \ldots & (|m_2|-1)|m_1|+c_{\varphi(m_1)}
\end{array}$$

Toate numerele întregi din noul tablou sînt prime cu m_1. Pentru a extrage din noul tablou numerele prime cu m este suficient să extragem numerele prime cu m_2, deoarece cele care nu sînt prime cu m_2 nu sînt prime nici cu m avînd $m=m_1m_2$, iar cele care sînt prime cu m sînt prime și cu m_1 și cu m_2.

Numărul numerelor prime cu m_2 din noul tablou îl determinăm în felul următor. Numerele întregi situate în aceeași coloană din noul tablou formează un sistem complet de resturi modulo m_2, deoarece ele sînt de forma $|m_1|\cdot 0+c_i$, $|m_1|\cdot 1+c_i, \ldots, |m_1|(|m_2|-1)+c_i$, unde $|m_1|$ este prim cu m_2, avînd $(m_1, m_2)\cong 1$, c_i este un număr întreg, putînd fi $c_1, c_2, \ldots, c_{\varphi(m_1)}$, iar $0, 1, \ldots, |m_2|-1$ constituie un sistem complet de resturi modulo m_2. Deci în fiecare coloană se află un număr $\varphi(m_2)$ de numere întregi prime cu m_2, aceste numere întregi constituind un sistem redus de

resturi modulo m_2. În noul tablou se află deci $\varphi(m_1)\varphi(m_2)$ numere întregi prime cu m_2 care în același timp sînt toate numerele prime cu m, din vechiul tablou, al căror număr este egal cu $\varphi(m)$, deci

$$\varphi(m)=\varphi(m_1)\varphi(m_2)$$

dacă $m\neq 0$, $m=m_1m_2$ și $(m_1, m_2)\cong 1$.

Dacă $m=0$, iar $m=m_1m_2$ și $(m_1,m_2)\cong 1$, atunci $m_1=0$, iar $m_2=\pm 1$ sau $m_2=0$ iar $m_1=\pm 1$. Dar

$$2=\varphi(0)=\varphi(0)\varphi(\pm 1)=2\cdot 1,$$

$$2=\varphi(0)=\varphi(\pm 1)\varphi(0)=1\cdot 2,$$

deci teorema este demonstrată în toate cazurile care se pot prezenta.

Exemplu. $m=21$, $m_1=3$, $m_2=7$. Avem $21=3\cdot 7$ și $(3, 7)\cong 1$. În sistemul complet de resturi modulo 21, anume în 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20 numerele întregi 1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20 formează un sistem redus de resturi modulo 21, deci $\varphi(21)=12$. În tabloul

$$\begin{array}{rrr}
1 & 2 & 3 \\
4 & 5 & 6 \\
7 & 8 & 9 \\
10 & 11 & 12 \\
13 & 14 & 15 \\
16 & 17 & 18 \\
19 & 20 & 21
\end{array}$$

numerele întregi 1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20 sînt repartizate cîte $\varphi(7)=6$ în prima și a doua coloană, deci în $\varphi(3)=2$ coloane, în prima coloană aflîndu-se 1, 4, 10, 13, 16, 19, iar în a doua coloană aflîndu-se 2, 5, 8, 11, 17, 20. Deci $\varphi(21)=\varphi(3)\varphi(7)$. Că avem $\varphi(3)=2$ și $\varphi(7)=6$, acest lucru se stabilește formînd cîte un sistem complet de resturi pentru fiecare din modulele 3 și 7 și extrăgînd apoi din ele sistemul corespunzător redus de resturi modulo m.

Teoremă. *Dacă* $m=\varepsilon p^\alpha$, *unde* $\varepsilon=\pm 1$, *iar* p *este un număr prim pozitiv,* α *fiind un număr natural, avem*

$$\varphi(m)=p^\alpha-p^{\alpha-1}=p^{\alpha-1}(p-1).$$

Demonstrație. Luăm numerele naturale mai mici sau cel mult egale cu $|m|$, unde $m=\varepsilon p^{\alpha}$, care formează un sistem complet de resturi modulo m, deoarece sînt $|m|$ numere întregi consecutive. Numerele neprime cu m din acest sistem se divid cu p. Într-adevăr, dacă c este neprim cu m, atunci c este neprim și cu p, deoarece dacă c ar fi prim cu p, atunci ar fi prim și cu $m=\varepsilon p^{\alpha}$, numărul εp^{α} fiind produs de numere ε, $\underbrace{p,\ldots,p}_{\text{de } \alpha \text{ ori}}$ prime cu c. Mai departe, c fiind neprim cu p se divide cu p, p fiind număr prim. Numai numerele neprime cu m din sistemul complet de resturi modulo m se divid cu p, deoarece dacă un număr întreg c se divide cu p, atunci $p|c$, $p|\varepsilon p^{\alpha}$ și deci p divide și pe cel mai mare divizor comun al lui c și m care pentru acest motiv nu poate fi asociat cu 1. Eliminînd din sistemul complet de resturi modulo m considerat, care are $|m|=p^{\alpha}$ elemente, numerele întregi divizibile cu p care sînt

$$1\cdot p,\ 2\cdot p,\ \ldots,\ p^{\alpha-1}\cdot p=|m|,$$

al căror număr este deci $p^{\alpha-1}$, obținem un sistem redus de resturi modulo $m=\varepsilon p^{\alpha}$ care are un număr de elemente egal cu $p^{\alpha}-p^{\alpha-1}$, deci

$$\varphi(\varepsilon p^{\alpha})=p^{\alpha}-p^{\alpha-1}=p^{\alpha-1}(p-1),$$

dacă p este un număr prim pozitiv și α este un număr natural.

Teoremă. *Dacă* $m=\varepsilon p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_r^{\alpha_r}$, *unde* $\varepsilon=\pm 1$, $0<p_1<p_2<\ldots<p_r$, $p_1, p_2, \ldots, p_r$ *fiind numere prime, iar* $\alpha_1, \alpha_2, \ldots, \alpha_r$ *sînt numere naturale, atunci*

$$\varphi(m)=p_1^{\alpha_1-1}p_2^{\alpha_2-1}\ldots p_r^{\alpha_r-1}(p_1-1)(p_2-1)\ldots(p_r-1).$$

Demonstrație.

$\varphi(m)=\varphi(\varepsilon p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_r^{\alpha_r})=\varphi(\varepsilon)\varphi(p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_r^{\alpha_r})$, deoarece $(\varepsilon, p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_r^{\alpha_r})\cong 1$, avînd $\varepsilon=\pm 1$. Deci $\varphi(m)=\varphi(p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_r^{\alpha_r})$, deoarece $\varphi(\varepsilon)=\varphi(\pm 1)=1$. Apoi

$$\varphi(m)=\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}\ldots p_r^{\alpha_r}),$$

deoarece

$$(p_1^{\alpha_1},\ p_2^{\alpha_2}\ldots p_r^{\alpha_r})\cong 1,$$

p_1 fiind număr prim neasociat cu nici unul dintre numerele prime $p_2, \ldots, p_r$, ceea ce conduce la $p_1\nmid p_2^{\alpha_2}\ldots p_r^{\alpha_r}$, deci $(p_1, p_2^{\alpha_2}\ldots p_r^{\alpha_r})\cong 1$,

deci $(p_1^{\alpha_1}, p_2^{\alpha_2}\ldots p_r^{\alpha_r})\cong 1$. Continuînd în același mod, obținem

$$\varphi(m)=\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\ldots\varphi(p_r^{\alpha_r})$$

și, deoarece $0<p_1$ etc., rezultă

$$\varphi(m)=(p^{\alpha_1}-p_1^{\alpha_1-1})(p_2^{\alpha_2}-p_2^{\alpha_2-1})\ldots(p_r^{\alpha_r}-p_r^{\alpha_r-1}),$$

de unde rezultă formula dată în enunțul teoremei.

Exemplu. $m=-50=-2\cdot 5^2$, $\varphi(-50)=2\cdot 5^1(2-1)(5-1)=5\cdot 4=20$.

4.4. Teoremele lui Euler, Fermat și Wilson

Teorema lui Euler. *Pentru orice număr întreg* a *prim cu un număr întreg* m *avem*

$$a^{\varphi(m)}\equiv 1 \pmod m.$$

Demonstrație. Fie $c_1, c_2, \ldots, c_{\varphi(m)}$ un sistem redus de resturi modulo m. Atunci $ac_1, ac_2, \ldots, ac_{\varphi(m)}$ este, de asemenea, un sistem redus de resturi modulo m, deoarece a este prim cu m.

Fiecărui ac din $ac_1, ac_2, \ldots, ac_{\varphi(m)}$ îi corespunde numai un c' din $c_1, c_2, \ldots, c_{\varphi(m)}$ care reprezintă aceeași clasă de resturi modulo m. Notînd cu c_i' acel număr întreg care îi corespunde lui ac_i, unde $1\leqslant i\leqslant\varphi(m)$, vom avea

$$ac_i\equiv c_i' \pmod m,$$

deci

$$a^{\varphi(m)}c_1c_2\ldots c_{\varphi(m)}\equiv c_1c_2\ldots c_{\varphi(m)} \pmod m,$$

deoarece $c_1'c_2'\ldots c'_{\varphi(m)}=c_1c_2\ldots c_{\varphi(m)}$, deci

$$a^{\varphi(m)}\equiv 1 \pmod m,$$

pentru că $c_1c_2\ldots c_{\varphi(m)}$ este prim cu m, fiecare $c_1, c_2, \ldots, c_{\varphi(m)}$ fiind prim cu m.

Exemplu. $a=6$, $m=25$. Avem $\varphi(m)=5(5-1)=20$ și $(a, m)\cong 1$, deci

$$6^{20}\equiv 1 \pmod{25},$$

ceea ce poate fi stabilit și astfel $6^{20} \equiv (6^2)^{10} \equiv 36^{10} \equiv 11^{10} \equiv (11^2)^5 \equiv$ $\equiv 121^5 \equiv (-4)^5 \equiv -2^{10} \equiv -1024 \equiv 1 \pmod{25}$.

Mica teoremă a lui Fermat. *Pentru orice număr întreg a care nu se divide cu un număr prim p, $p>0$, avem*

$$a^{p-1} \equiv 1 \pmod{\pm p}.$$

Demonstrație. Dacă a nu se divide cu un număr prim p, atunci a este prim cu $\pm p$, conform unei proprietăți a numerelor prime din 3.6, ținînd seama și de aceea că $-p$ este prim dacă și numai dacă p este prim. Atunci, conform teoremei lui Euler, avem

$$a^{\varphi(p)} \equiv 1 \pmod{p},$$

unde $\varphi(p) = p-1$.

Exemplu. $a=9$, $p=5$. Avem $p-1=5-1=4$ și $p \nmid a$, deci

$$9^4 \equiv 1 \pmod{5},$$

ceea ce poate fi stabilit și astfel $9^4 \equiv 3^8 \equiv (3^4)^2 \equiv 81^2 \equiv 1^2 \equiv 1 \pmod{5}$.

Observație. Mica teoremă a lui Fermat poate fi formulată și astfel.

Pentru orice număr întreg a avem

$$a^p \equiv a \pmod{\pm p},$$

p fiind număr prim, $p>0$.

Într-adevăr, dacă $p \nmid a$, atunci $a^{p-1} \equiv 1 \pmod{\pm p}$, deci $a \cdot a^{p-1} \equiv a \pmod{\pm p}$ sau $a^p \equiv a \pmod{\pm p}$, iar dacă $p \mid a$, avem $p \mid a^p$, deci $p \mid a^p - a$, de unde $a^p \equiv a \pmod{\pm p}$. Reciproc, dacă, $p \nmid a$, din $a^p \equiv a \pmod{\pm p}$ sau $p \mid a^p - a$ deducem $p \mid a(a^{p-1}-1)$, deci $p \mid a^{p-1}-1$ deoarece p este prim și $p \nmid a$, deci $a^{p-1} \equiv 1 \pmod{\pm p}$.

Teorema lui Wilson. *Dacă p este număr prim $p>0$, avem*

$$(p-1)! \equiv -1 \pmod{\pm p}.$$

Observație. Avem $(p-1)! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1)$, iar $(p-1)!$ se numește *$(p-1)$-factorial.*

Prima demonstrație. Fie $c_1, c_2, \ldots, c_{\varphi(p)}$ un sistem redus de resturi modulo p. Dacă c_i este unul din $c_1, c_2, \ldots, c_{\varphi(p)}$ atunci $c_i c_1, c_i c_2, \ldots, c_i c_{\varphi(p)}$ este un sistem redus de resturi modulo p, deoarece c_i este prim cu p. Deci fiecărui c din $c_1, c_2, \ldots, c_{\varphi(p)}$ îi corespunde numai un c' din $c_1, c_2, \ldots, c_{\varphi(p)}$ astfel încît

$$cc' \equiv 1 \pmod{p},$$

deoarece numai un număr întreg din $c_i c_1, c_i c_2, \ldots, c_i c_{\varphi(p)}$ reprezintă clasa modulo p, reprezentată de 1. Și fiecărui c' din $c_1, c_2, \ldots, c_{\varphi(p)}$ îi corespunde numai un c din $c_1, c_2, \ldots, c_{\varphi(p)}$ astfel încît

$$cc' \equiv 1 \pmod{p},$$

deoarece această congruență poate fi scrisă și sub forma

$$c'c \equiv 1 \pmod{p}.$$

Înmulțind membru cu membru aceste congruențe, luînd numai una din congruențele $cc' \equiv 1 \pmod{p}$, $c'c \equiv 1 \pmod{p}$ în cazul cînd $c' \neq c$, obținem

$$c_1 c_2 \ldots c_{\varphi(p)} \cdot a \equiv 1 \pmod{p},$$

unde a reprezintă produsul tuturor acelor c pentru care $c' = c$, deoarece, în acest caz, avem

$$c^2 \equiv 1 \pmod{p}.$$

Numerele c din $c_1, c_2, \ldots, c_{\varphi(p)}$ pentru care

$$c^2 \equiv 1 \pmod{p}$$

sînt astfel încît $p \mid c^2 - 1$, deci $p \mid (c-1)(c+1)$, de unde sau $p \mid c-1$, deci

$$c \equiv 1 \pmod{p}$$

sau $p \mid c+1$, deci

$$c \equiv -1 \pmod{p},$$

deoarece p este prim. Avem două astfel de numere, deoarece 1 și -1 sînt necongruente modulo p în cazul cînd $p \neq 2$, fiindcă dacă $1 \equiv -1 \pmod{p}$, atunci $2 \equiv 0 \pmod{p}$, deci $p \mid 2$, de unde $p = 2$, pentru că p este prim, ceea ce se contrazice cu $p \neq 2$. Deci pentru $p \neq 2$

$$a \equiv -1 \pmod{p}$$

și deci

$$c_1 c_2 \ldots c_{\varphi(p)} \equiv -1 \pmod{p}.$$

Însă 1, 2, 3, ..., $p-1$ formează un sistem redus de resturi modulo p, deoarece 0, 1, 2, 3, ..., $p-1$ este un sistem complet de resturi modulo p și numai 0 nu este prim cu p, toate cele-

lalte numere întregi 1, 2, 3, ..., $p-1$ fiind prime cu p, deoarece sînt mai mici ca p și ca urmare nu se divid cu p. Așadar

$$1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \equiv -1 \pmod{\pm p}.$$

Teorema lui Wilson este adevărată și în cazul cînd $p=2$, deoarece $2-1=1$, $1!=1$, iar $1 \equiv -1 \pmod{\pm 2}$.

Exemplu. Fie $p=11$. Pentru numerele naturale 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 avem

$$\begin{aligned}
1 \cdot 1 &\equiv 1 \pmod{-11},\\
2 \cdot 6 &\equiv 1 \pmod{-11},\\
3 \cdot 4 &\equiv 1 \pmod{-11},\\
4 \cdot 3 &\equiv 1 \pmod{-11},\\
5 \cdot 9 &\equiv 1 \pmod{-11},\\
6 \cdot 2 &\equiv 1 \pmod{-11},\\
7 \cdot 8 &\equiv 1 \pmod{-11},\\
8 \cdot 7 &\equiv 1 \pmod{-11},\\
9 \cdot 5 &\equiv 1 \pmod{-11},\\
10 \cdot 10 &\equiv 1 \pmod{-11},
\end{aligned}$$

deci $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot (1 \cdot 10) \equiv 1 \pmod{-11}$. Dar $1 \cdot 10 \equiv -1 \pmod{-11}$, prin urmare $10! \equiv -1 \pmod{-11}$.

A doua demonstrație. Să considerăm polinomul cu coeficienții întregi

$$f(x) = (x-1)(x-2)\ldots(x-(p-1)) - (x^{p-1}-1),$$

unde p este număr prim, $p>0$. Acest polinom are gradul $p-2$ dacă $p \neq 2$, iar dacă $p=2$, polinomul $f(x)$ este nul. În cazul $p=2$ teorema lui Wilson este adevărată așa cum am văzut la sfîrșitul primei demonstrații.

Dacă $p \neq 2$, se constată că congruența

$$f(x) \equiv 0 \pmod{p}$$

admite ca soluții pe 1, 2, ..., $p-1$, deoarece, pentru orice număr întreg i, $1 \leqslant i \leqslant p-1$, avem

$$(i-1)(i-2)\ldots(i-(p-1)) = 0,$$

iar $i^{p-1} \equiv 1 \pmod{p}$, conform teoremei lui Fermat. Deci congruența

$$f(x) \equiv 0 \pmod{p}$$

are $p-1$ soluții distincte și cum gradul $p-2$ al polinomului $f(x)$ este mai mic decît numărul soluțiilor distincte ale congruenței $f(x) \equiv 0 \pmod{p}$ înseamnă că coeficienții polinomului $f(x)$ se divid cu p. În particular, termenul liber al polinomului $f(x)$ se divide cu p. Termenul liber al polinomului $f(x)$ este

$$(-1)^{p-1} 1 \cdot 2 \cdot \ldots \cdot (p-1) + 1,$$

deci

$$p \mid (-1)^{p-1} 1 \cdot 2 \cdot \ldots \cdot (p-1) + 1,$$

prin urmare

$$(p-1)! \equiv -1 \pmod{\pm p},$$

deoarece $(-1)^{p-1}=1$, p fiind prim și diferit de 2, deci impar.

Observație. Teorema lui Wilson are și o reciprocă, care se enunță în felul următor.

Dacă pentru un număr întreg p avem relația

$$(p-1)! \equiv -1 \pmod{\pm p},$$

iar $p>0$, $p \neq 1$, atunci p este prim.

Într-adevăr, dacă p n-ar fi prim, avînd în vedere că $p \neq 1$, ar avea un divizor propriu q care poate fi ales pozitiv. Atunci am avea $1<q<p$, deoarece $p>0$, sau $2 \leqslant q \leqslant p-1$ și deci am avea $q \mid (p-1)!$, iar din $(p-1)! \equiv -1 \pmod{\pm p}$ și $q \mid p$ am deduce $(p-1)! \equiv -1 \pmod{q}$, deci $q \mid -1$, ceea ce nu este posibil, deoarece q este divizor propriu al lui p. Ca să nu avem această contrazicere, trebuie ca p să fie prim.

Teorema lui Wilson ne dă deci posibilitatea de a constata dacă un număr întreg p este prim sau nu, după cum $p \mid (p-1)!+1$ sau $p \nmid (p-1)!+1$, dar această posibilitate nu poate fi folosită, din cauză că numărul întreg $(p-1)!+1$ este foarte mare.

Capitolul 5

RĂDĂCINI PRIMITIVE

5.1. Ordinul unei clase de resturi modulo m, primă cu modulul

Definiție. *Ordinul unei clase de resturi modulo m, primă cu modulul, reprezentată de un număr întreg a este un număr natural δ pentru care*

$$a^{\delta} \equiv 1 \pmod{m},$$

$$a^{\mu} \not\equiv 1 \pmod{m}$$

oricare ar fi numărul întreg μ astfel încît $0<\mu<\delta$.

Observație. Deoarece definiția ordinului unei clase de resturi modulo m, primă cu modulul, se dă cu ajutorul unui reprezentant al clasei considerate, acest ordin se mai numește *exponentul lui care aparține un număr întreg prim cu modulul.*

Ordinul unei clase de resturi modulo m, primă cu modulul, reprezentată de numărul întreg a există, deoarece, conform teoremei lui Euler, avem

$$a^{\varphi(m)} \equiv 1 \pmod{m},$$

unde $\varphi(m)$ este un număr natural. Deci pe δ putem să-l determinăm luînd cel mai mic număr natural dintre numerele naturale ν pentru care

$$1 \leqslant \nu \leqslant \varphi(m),$$

$$a^{\nu} \equiv 1 \pmod{m}.$$

Ordinul unei clase de resturi modulo m, primă cu modulul, este unic, adică nu depinde de reprezentantul clasei. Într-adevăr, dacă $b \equiv a \pmod{m}$, avem $b^{\delta} \equiv a^{\delta} \equiv 1 \pmod{m}$ și $b^{\mu} \not\equiv 1 \pmod{m}$, oricare ar fi numărul întreg μ astfel încît $0<\mu<\delta$, deoarece dacă $b^{\mu} \equiv 1 \pmod{m}$, atunci și $a^{\mu} \equiv b^{\mu} \equiv 1 \pmod{m}$, ceea ce este contradictoriu.

Ordinul unei clase de resturi modulo m, primă cu modulul, are următoarele proprietăți:

(1) *Dacă a aparține unei clase de resturi modulo m, primă cu modulul, de ordin δ, atunci numerele*

$$a^0, a^1, \ldots, a^{\delta-1}$$

sînt necongruente două cîte două modulo m.

Demonstrație. Să presupunem prin absurd că

$$a^h \equiv a^k \pmod{m},$$

unde $0 \leqslant h \leqslant \delta-1$, $0 \leqslant k \leqslant \delta-1$, $h \neq k$. Unul dintre numerele h, k trebuie să fie mai mare decît celălalt. Să presupunem că $h>k$. Atunci, avînd $(a, m) \cong 1$ deci $(a^k, m) \cong 1$ rezultă

$$a^{h-k} \equiv 1 \pmod{m}.$$

Dar $0<h-k<\delta$, deoarece $h>k$, deci $h-k>0$ și deoarece $0 \leqslant h \leqslant \delta-1$, $0 \leqslant k \leqslant \delta-1$ deci $h-k \leqslant h-k+k=h \leqslant \delta-1<\delta$. Însă

$$a^{h-k} \equiv 1 \pmod{m}$$

și $0<h-k<\delta$ contrazice faptul că δ este ordinul clasei de resturi modulo m, primă cu modulul, reprezentată de a. Cu aceasta, proprietatea este demonstrată.

(2) *Dacă a aparține unei clase de resturi modulo m, primă cu modulul, de ordin δ, atunci*

$$a^{\alpha} \equiv a^{\alpha'} \pmod{m}$$

este echivalentă cu

$$\gamma \equiv \gamma' \pmod{\delta},$$

unde γ *și* γ' *sînt numere întregi.*

Demonstrație. Fie $a^\gamma \equiv a^{\gamma'} \pmod{m}$. Deoarece $\delta \neq 0$, fiind un număr natural, prin aplicarea teoremei împărțirii întregi obținem

$$\gamma = \delta q + r, \quad 0 \leqslant r < \delta,$$

$$\gamma' = \delta q' + r', \quad 0 \leqslant r' < \delta.$$

Avem $a^\gamma \equiv a^{\delta q + r} \equiv (a^\delta)^q a^r \equiv 1^q a^r \equiv a^r \pmod{m}$. Tot astfel $a^{\gamma'} \equiv a^{r'} \pmod{m}$, deci din $a^\gamma \equiv a^{\gamma'} \pmod{m}$ rezultă

$$a^r \equiv a^{r'} \pmod{m}.$$

Din cauză că $0 \leqslant r < \delta$, deci $0 \leqslant r \leqslant \delta - 1$ și $0 \leqslant r' < \delta$, deci $0 \leqslant r' \leqslant \delta - 1$, conform proprietății (1) rezultă

$$r = r'.$$

Conform celei de-a doua definiții a relației de congruență obținem

$$\gamma \equiv \gamma' \pmod{\delta}.$$

Reciproc, fie $\gamma \equiv \gamma' \pmod{\delta}$. Deci $\delta \mid \gamma - \gamma'$, deci $\gamma - \gamma' = \delta q$ sau $\gamma = \gamma' + \delta q$. Atunci

$$a^\gamma \equiv a^{\gamma' + \delta q} \equiv a^{\gamma'} (a^\delta)^q \equiv a^{\gamma'} \cdot 1^q \equiv a^{\gamma'} \pmod{m}.$$

(3) *Dacă* a *aparține unei clase de resturi modulo* m, *primă cu modulul, de ordin* δ, *atunci*

$$a^\gamma \equiv 1 \pmod{m}$$

este echivalentă cu $\delta \mid \gamma$, γ *fiind un număr întreg și în particular* $\delta \mid \varphi(m)$.

Demonstrație. Conform proprietății (2), $a^\gamma \equiv 1 \pmod{m}$, scrisă sub forma $a^\gamma \equiv a^0 \pmod{m}$, este echivalentă cu $\gamma \equiv 0 \pmod{\delta}$, deci cu $\delta \mid \gamma - 0$, deci cu $\delta \mid \gamma$.

În particular avem $a^{\varphi(m)} \equiv 1 \pmod{m}$, deci $\delta \mid \varphi(m)$.

(4) *Dacă* x *aparține unei clase de resturi modulo* m, *primă cu modulul, de ordin* ab, *atunci* x^a *aparține unei clase de resturi modulo* m, *primă cu modulul, de ordin* b, a *și* b *fiind numere naturale.*

Demonstrație. Deoarece x aparține unei clase de resturi modulo m, primă cu modulul, avem $(x, m) \cong 1$, deci $(x^a, m) \cong 1$ și deci x^a aparține unei clase de resturi modulo m, primă cu modulul.

Fie δ ordinul clasei de resturi modulo m, primă cu modulul, pe care o reprezintă x^a. Avem deci

$$(x^a)^\delta \equiv 1 \pmod{m}.$$

Dacă scriem această congruență sub forma $x^{a\delta} \equiv 1 \pmod{m}$, atunci $ab \mid a\delta$, deoarece ab este ordinul clasei de resturi modulo m, primă cu modulul reprezentată de x. Deoarece $ab \neq 0$, ab fiind un număr natural, avem $a \neq 0$, deci din $ab \mid a\delta$ deducem $b \mid \delta$.

Din cauză că ab este ordinul clasei de resturi modulo m, primă cu modulul, reprezentată de x, putem scrie

$$x^{ab} \equiv 1 \pmod{m}.$$

Dacă scriem această congruență sub forma

$$(x^a)^b \equiv 1 \pmod{m},$$

atunci $\delta \mid b$, deoarece δ este ordinul clasei de resturi modulo m primă cu modulul, reprezentată de x^a. Avînd $b \mid \delta$ și $\delta \mid b$, avem $\delta = b$, atît δ cît și b fiind numere naturale. Cu aceasta proprietatea este dovedită.

(5) *Dacă* x *aparține unei clase de resturi modulo* m, *primă cu modulul, de ordin* a, *iar* y *aparține unei clase de resturi modulo* m, *primă cu modulul, de ordin* b, *iar* $(a, b) \cong 1$, *atunci* xy *aparține unei clase de resturi modulo* m, *primă cu modulul, de ordin* ab.

Demonstrație. Deoarece x și y aparțin unor clase de resturi modulo m, prime cu modulul, avem $(x, m) \cong 1$, $(y, m) \cong 1$, deci $(xy, m) \cong 1$, deci xy aparține unei clase de resturi modulo m, primă cu modulul.

Fie δ ordinul clasei de resturi modulo m, primă cu modulul, pe care o reprezintă xy. Avem deci

$$(xy)^\delta \equiv 1 \pmod{m}.$$

De aici rezultă că $(xy)^{a\delta} \equiv 1 \pmod{m}$ și $(xy)^{b\delta} \equiv 1 \pmod{m}$. Din $(xy)^{a\delta} \equiv 1 \pmod{m}$ rezultă că $1 \equiv (xy)^{a\delta} \equiv x^{a\delta} y^{a\delta} \equiv (x^a)^\delta y^{a\delta} \equiv 1^\delta y^{a\delta} \equiv y^{a\delta} \pmod{m}$, deci $y^{a\delta} \equiv 1 \pmod{m}$, a fiind ordinul clasei de resturi modulo m, primă cu modulul, reprezentată de x. Din

$y^{a\delta} \equiv 1 \pmod m$ rezultă $b \mid a\delta$, deoarece b este ordinul clasei de resturi modulo m, primă cu modulul, reprezentată de y. Din $b \mid a\delta$ și $(a, b) \cong 1$ rezultă $b \mid \delta$.

Din $(xy)^{b\delta} \equiv 1 \pmod m$ rezultă $1 \equiv (xy)^{b\delta} \equiv x^{b\delta} y^{b\delta} \equiv x^{b\delta} (y^b)^\delta \equiv x^{b\delta} 1^\delta \equiv x^{b\delta} \pmod m$, deci $x^{b\delta} \equiv 1 \pmod m$, b fiind ordinul clasei de resturi modulo m, primă cu modulul, reprezentată de y. Din $x^{b\delta} \equiv 1 \pmod m$ rezultă $a \mid b\delta$, deoarece a este ordinul clasei de resturi modulo m, primă cu modulul, reprezentată de x. Din $a \mid b\delta$ și $(a, b) \cong 1$ rezultă $a \mid \delta$.

Din $a \mid \delta$ și $b \mid \delta$ rezultă $[a, b] \mid \delta$. Dar $[a,b] \cong \frac{ab}{(a,b)} \cong ab$, deci $ab \mid \delta$. Cu $[a, b]$ am notat cel mai mic multiplu comun al numerelor întregi a și b.

Acum, din cauză că a este ordinul clasei de resturi modulo m, primă cu modulul, reprezentată de x și din cauză că b este ordinul clasei de resturi modulo m, primă cu modulul, reprezentată de y avem $x^a \equiv 1 \pmod m$, $y^b \equiv 1 \pmod m$, deci $(x^a)^b \equiv 1 \pmod m$, $(y^b)^a \equiv 1 \pmod m$, deci $x^{ab} \equiv 1 \pmod m$, $y^{ab} \equiv 1 \pmod m$, deci $x^{ab} y^{ab} \equiv 1 \pmod m$, deci $(xy)^{ab} \equiv 1 \pmod m$. Avem $\delta \mid ab$ din cauză că δ este ordinul clasei de resturi modulo m, primă cu modulul, reprezentată de xy. Avînd $ab \mid \delta$ și $\delta \mid ab$ obținem $\delta = ab$, ambele numere δ și ab fiind naturale.

Observație. Noțiunea de ordin al unei clase de resturi modulo m, primă cu modulul, provine din teoria grupurilor. Anume dacă avem un grup G și a este un element al acestui grup, atunci ordinul elementului a este cel mai mic număr natural n astfel încît

$$a^n = e,$$

unde e este elementul neutru din grup față de operația de compunere din grupul considerat, iar a^n înseamnă a^{n-1} compus cu a, unde $a^0 = e$. În cazul claselor de resturi modulo m, prime cu modulul, am demonstrat că ele formează grup față de operația de înmulțire a claselor de resturi modulo m. În acest caz δ este ordinul unei clase C_a modulo m, primă cu modulul, deoarece din $a^\delta \equiv 1 \pmod m$ rezultă $C_a{}^\delta = C_1$, adică $(C_a)^\delta = C_1$, avînd $C_a{}^\delta = (C_a)^\delta$, δ fiind cel mai mic număr natural n cu proprietatea $(C_a)^n = C_1$ ca urmare a faptului că din $a^\mu \not\equiv 1 \pmod m$ rezultă $(C_a)^\mu \neq C_1$ oricare ar fi numărul întreg μ astfel încît $0 < \mu < \delta$, elementul neutru din grupul multiplicativ al claselor de resturi modulo m, prime cu modulul, fiind C_1.

Denumirea de exponent la care aparține un număr întreg dintr-o clasă de resturi modulo m, primă cu modulul, este o denumire veche din teoria numerelor utilizată pînă în momentul în care a apărut noțiunea de ordin, pentru că atunci s-a văzut că această noțiune se atașează nu numerelor întregi care fac parte dintr-o congruență, ci se atașează claselor de resturi modulo m, prime cu modulul.

Am văzut că numărul de elemente din grupul multiplicativ al claselor de resturi modulo m, prime cu modulul, este $\varphi(m)$. Deci acest grup are un număr finit de elemente și de aceea se numește grup finit. Am demonstrat că ordinul δ al unei clase de resturi C_a, unde $(a, m) \cong 1$, divide pe $\varphi(m)$. În teoria grupurilor numărul de elemente ale unui grup finit se numește ordinul grupului. Deci $\delta \mid \varphi(m)$ înseamnă că ordinele elementelor divid ordinul grupului. Această proprietate este adevărată pentru orice grup finit constituind teorema lui Lagrange.

5.2. Rădăcini primitive modulo m

Definiție. *Un număr întreg a prim cu m se numește rădăcină primitivă modulo m, dacă aparține unei clase de resturi modulo m, primă cu modulul, de ordin $\varphi(m)$.*

Cu alte cuvinte, un număr întreg a prim cu m se numește rădăcină primitivă modulo m, dacă

$$a^{\varphi(m)} \equiv 1 \pmod m,$$
$$a^\mu \not\equiv 1 \pmod m,$$

oricare ar fi numărul întreg μ astfel încît $0 < \mu < \varphi(m)$.

Teoremă. *Dacă $(a, 2) \cong 1$ și α este număr întreg cel puțin egal cu 3, atunci*

$$a^{\frac{1}{2}\varphi(\pm 2^\alpha)} \equiv 1 \pmod{\pm 2^\alpha}.$$

Demonstrație. Dacă $(a, 2) \cong 1$ atunci $2 \nmid a$, deoarece 2 este număr prim. Aplicînd teorema împărțirii întregi, obținem, în acest caz

$$a = 2t + 1.$$

Prin ridicare la pătrat obținem

$$a^2=4t^2+4t+1=1+4t(t+1).$$

Unul din cele două numere întregi consecutive t, $t+1$ se divide cu 2, deci $t(t+1)=2t_1$, deci

$$a^2=1+8t_1.$$

Acest lucru îl vom scrie sub forma

$$a^{2^1}=1+2^3t_1.$$

Această relație ne sugerează să demonstrăm prin inducție completă relația

$$a^{2^n}=1+2^{n+2}t_n,$$

în care n este un număr natural. Relația scrisă este adevărată pentru $n=1$. Să o presupunem adevărată pentru $n=i$. Avem deci $a^{2^i}=1+2^{i+2}t_i$. Atunci $(a^{2^i})^2=(1+2^{i+2}t_i)^2$, deci $a^{2^{i+2}}=1+2\cdot 2^{i+2}t_i+(2^{i+2})^2t_i^2$ sau $a^{2^{i+1}}=1+2^{i+3}t_i+2^{2i+4}t_i^2=1+2^{i+3}(t_i+2^{i+1}t_i^2)=1+2^{i+3}t_{i+1}$, unde am notat $t_{i+1}=t_i+2^{i+1}t_i^2$. Proprietatea este deci adevărată și pentru $n=i+1$, deci este adevărată pentru orice n număr natural.

Dacă luăm $n=\alpha-2$ cu condiția $n\geqslant 1$, adică $\alpha-2\geqslant 1$, obținem

$$a^{2^{\alpha-2}}=1+2^\alpha t_{\alpha-2},$$

$$a^{\frac{1}{2}\varphi(\pm 2^\alpha)}\equiv 1 \pmod{\pm 2^\alpha},$$

deoarece dacă $\alpha\geqslant 3$ avem $\frac{1}{2}\varphi(\pm 2^\alpha)=\frac{1}{2}2^{\alpha-1}=2^{\alpha-2}$, unde $\alpha-2\geqslant 1$.

Consecință. Nu există rădăcini primitive modulo $\pm 2^\alpha$, unde $\alpha\geqslant 3$, α fiind număr natural, deoarece dacă $(a, \pm 2^\alpha)\cong 1$ avem $(a, 2)\cong 1$, deci

$$a^{\frac{1}{2}\varphi(\pm 2^\alpha)}\equiv 1 \pmod{\pm 2^\alpha},$$

cu $0<\frac{1}{2}\varphi(\pm 2^\alpha)<\varphi(\pm 2^\alpha)$.

Teoremă. *Pot exista rădăcini primitive modulo m, numai dacă $m=0$ sau $m=\pm 2^\alpha$ sau $m=\pm p^\beta$ sau $m=\pm 2p^\beta$, unde p este număr prim pozitiv diferit de 2, $\alpha=0, 1, 2$, iar β este un număr natural.*

Demonstrație. Fie $m\neq 0$ și $m=\varepsilon 2^\alpha p_1^{\alpha_1}\ldots p_r^{\alpha_r}$, unde $\varepsilon=\pm 1$, $p_1, \ldots, p_r$ sînt numere prime pozitive diferite două cîte două și diferite de 2, iar $\alpha, \alpha_1, \ldots, \alpha_r$ sînt numere întregi nenegative.

Vom face următoarele notații:

$$\tau=\varphi(2^\alpha) \text{ dacă } 0\leqslant\alpha\leqslant 2 \text{ și } \tau=\frac{1}{2}\varphi(2^\alpha) \text{ dacă } \alpha>2,$$

$$c_1=\varphi(p_1^{\alpha_1}),\ c_2=\varphi(p_2^{\alpha_2}),\ \ldots,\ c_r=\varphi(p_r^{\alpha_r}).$$

Dacă $(a, m)\cong 1$, atunci $(a, 2^\alpha)\cong 1$, $(a, p_1^{\alpha_1})\cong 1, \ldots, (a, p_r^{\alpha_r})\cong 1$ și atunci, datorită teoremei lui Euler și a teoremei demonstrate mai sus, avem

$$a^\tau\equiv 1 \pmod{2^\alpha},$$
$$a^{c_1}\equiv 1 \pmod{p_1^{\alpha_1}},$$
$$\ldots\ldots\ldots\ldots$$
$$a^{c_r}\equiv 1 \pmod{p_r^{\alpha_r}}.$$

Fie acum $h\cong[\tau, c_1, c_2, \ldots, c_r]$, adică h este cel mai mic multiplu comun al numerelor întregi $\tau, c_1, c_2, \ldots, c_r$. Putem lua $h>0$, deoarece $h\neq 0$, ca urmare a faptului că $\tau\neq 0$, $c_1\neq 0$, $c_2\neq 0$, $\ldots$, $c_r\neq 0$, unde $c_1, c_2, \ldots, c_r$ sînt valorile indicatorilor lui Euler care sînt numere naturale, τ fiind și el valoarea indicatorului lui Euler sau această valoare împărțită cu 2. Avem deci $h=\tau\tau'$, $h=c_1c_1'$, $\ldots$, $h=c_rc_r'$, deci

$$a^{\tau\tau'}\equiv 1 \pmod{2^\alpha},$$
$$a^{c_1c_1'}\equiv 1^{c_1'} \pmod{p_1^{\alpha_1}},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$a^{c_rc_r'}\equiv 1^{c_r'} \pmod{p_r^{\alpha_r}},$$

deci

$$a^h\equiv 1 \pmod{2^\alpha},$$
$$a^h\equiv 1 \pmod{p_1^{\alpha_1}},$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$a^h\equiv 1 \pmod{p_r^{\alpha_r}},$$

așadar $2^\alpha \mid a^h-1$, $p_1^{\alpha_1} \mid a^h-1, \ldots, p_r^{\alpha_r} \mid a^h-1$, deci $[2^\alpha, p_1^{\alpha_1}, \ldots, p_r^{\alpha_r}] \mid a^h-1$. Dar $m \cong [2^\alpha, p_1^{\alpha_1}, \ldots, p_r^{\alpha_r}]$, pentru că numerele întregi 2^α, $p_1^{\alpha_1}, \ldots, p_r^{\alpha_r}$ sînt prime două cîte două. Prin urmare

$$m \mid a^h-1,$$

deci

$$a^h \equiv 1 \pmod{m}.$$

Avem $h \leqslant \varphi(m)$, deoarece $\varphi(m)=\varphi(2^\alpha)c_1c_2\ldots c_r$ în timp ce $h \cong [\tau, c_1, c_2, \ldots, c_r]$ și deci $h \mid \tau c_1c_2\ldots c_r$, deci $h \leqslant \tau c_1c_2\ldots c_r \leqslant \varphi(2^\alpha)c_1c_2\ldots c_r = \varphi(m)$.

Să luăm cazul cînd $\alpha>2$. Atunci $\tau = \frac{1}{2}\varphi(2^\alpha) < \varphi(2^\alpha)$, așadar

$$\tau c_1c_2\ldots c_r < \varphi(2^\alpha)c_1c_2\ldots c_r$$

deci

$$h<\varphi(m).$$

Fie acum $\alpha=2$ și cel puțin unul dintre $\alpha_1, \ldots, \alpha_r$ este cel puțin egal cu 1. Atunci dacă $\alpha_i \geqslant 1$ avem

$$\varphi(p_i^{\alpha_i}) = p_i^{\alpha_i-1}(p_i-1).$$

Deoarece $p_i-1=2q_i$ înseamnă că $\tau \mid \varphi(p_i^{\alpha_i})$, deoarece $\tau=\varphi(2^\alpha)=\varphi(2^2)=2$. Deci $\tau \mid c_1c_2\ldots c_r$. Dar și $c_1 \mid c_1c_2\ldots c_r, \ldots, c_r \mid c_1c_2\ldots c_r$, deci $h \mid c_1c_2\ldots c_r$, prin urmare

$$h \leqslant c_1c_2\ldots c_r < 2c_1c_2\ldots c_r = \varphi(m),$$

deci

$$h<\varphi(m).$$

Fie acum cel puțin doi dintre $\alpha_1, \ldots, \alpha_r$ cel puțin egali cu 1. Presupunem că $\alpha_i \geqslant 1$ și $\alpha_j \geqslant 1$, unde $i \neq j$. Deoarece $p_i-1=2q_i$, $p_j-1=2q_j$ înseamnă că $c_i \mid \frac{1}{2}c_ic_j$, $c_j \mid \frac{1}{2}c_ic_j$, pentru că $\frac{1}{2}c_ic_j = c_i\left(\frac{1}{2}c_j\right) = c_i\frac{1}{2}\varphi(p_j^{\alpha_j}) = c_i\frac{1}{2}p_j^{\alpha_j-1}(p_j-1) = c_ip_j^{\alpha_j-1}q_j = c_j\left(\frac{1}{2}c_i\right) = c_jp_i^{\alpha_i-1}q_i$. Deci $\tau \left| \frac{1}{2}\tau c_1\ldots c_r, c_1 \right| \frac{1}{2}\tau c_1\ldots c_r, \ldots, c_r \left| \frac{1}{2}\tau c_1\ldots c_r \right.$, așadar $h \left| \frac{1}{2}\tau c_1\ldots c_r \right.$, deci $h \leqslant \frac{1}{2}\tau c_1\ldots c_r \leqslant \frac{1}{2}\varphi(m) < \varphi(m)$,

deci

$$h<\varphi(m).$$

Am arătat deci că pentru $m \neq 0$,

$$m = \varepsilon 2^\alpha p_1^{\alpha_1} \ldots p_r^{\alpha_r}$$

avem $h<\varphi(m)$ în următoarele cazuri

(1) $\alpha>2$;

(2) $\alpha=2$ și cel puțin unul dintre $\alpha_1, \ldots, \alpha_r$ este cel puțin egal cu 1;

(3) cel puțin doi dintre $\alpha_1, \ldots, \alpha_r$ sînt cel puțin egali cu 1.

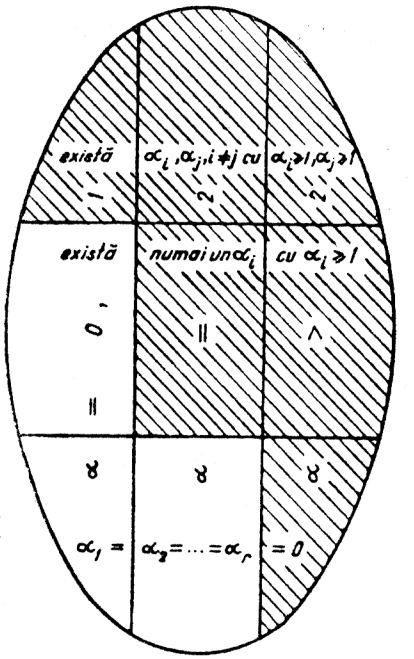


Fig 5.1.

În celelalte cazuri putem avea $h=\varphi(m)$. Pentru $m \neq 0$ celelalte cazuri sînt (vezi fig. 5.1. în care ariile corespunzătoare cazurilor de mai sus sînt hașurate):

(1) $\alpha \leqslant 2$ și toți $\alpha_1, \ldots, \alpha_r$ sînt egali cu 0;
(2) $\alpha = 0$ sau $\alpha = 1$ și numai unul dintre $\alpha_1, \ldots, \alpha_r$ este diferit de zero.

Referitor la cazurile în care putem avea $h = \varphi(m)$, cazul (1) corespunde la $m = \pm 2^\alpha$, $\alpha = 0, 1, 2$, iar cazul (2) corespunde la $m = \pm 2^\alpha p^\beta$, ceea ce pentru $\alpha = 0$ ne dă $m = \pm p^\beta$, iar pentru $\alpha = 1$ ne dă $m = \pm 2p^\beta$, β fiind un număr natural egal cu acela dintre $\alpha_1, \alpha_2, \ldots, \alpha_r$ care este diferit de zero și cu aceasta teorema este demonstrată.

5.3. Existența rădăcinilor primitive modulo m

În cele ce urmează vom arăta că există rădăcini primitive modulo m, dacă $m = 0$ sau $m = \pm 2^\alpha$ sau $m = \pm p^\beta$ sau $m = \pm 2p^\beta$, unde p este număr prim pozitiv diferit de 2, $\alpha = 0, 1, 2$, iar β este un număr natural.

Teoremă. *Există rădăcini primitive modulo p, unde p este număr prim.*

Demonstrație. Să luăm un sistem redus de resturi $c_1, c_2, \ldots c_{\varphi(p)}$ modulo p. Fie $\delta_1, \delta_2, \ldots, \delta_{\varphi(p)}$ ordinele claselor de resturi modulo p, reprezentate respectiv de $c_1, c_2, \ldots, c_{\varphi(p)}$. Fie $\tau \cong [\delta_1, \delta_2, \ldots, \delta_{\varphi(p)}]$. Deoarece $\delta_1, \delta_2, \ldots, \delta_{\varphi(p)}$ sînt numere naturale, putem să-l luăm pe τ pozitiv. Putem scrie

$$\tau = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r},$$

unde $p_1, p_2, \ldots, p_r$ sînt numere prime pozitive diferite două cîte două, iar $\alpha_1, \alpha_2, \ldots, \alpha_r$ sînt numere întregi nenegative.

Există printre $\delta_1, \delta_2, \ldots, \delta_{\varphi(p)}$ unul care să se dividă cu $p_i^{\alpha_i}$. Într-adevăr, dacă nici unul dintre $\delta_1, \delta_2, \ldots, \delta_{\varphi(p)}$ nu s-ar divide cu $p_i^{\alpha_i}$, atunci exponentul lui p_i în τ, care este cel mai mic multiplu comun al lui $\delta_1, \delta_2, \ldots, \delta_{\varphi(p)}$, ar fi mai mic decît α_i, deoarece cel mai mic multiplu comun este produsul factorilor primi comuni și necomuni la puterea cea mai mare. Vom nota cu δ_i' pe unul dintre $\delta_1, \delta_2, \ldots, \delta_{\varphi(p)}$ care se divide cu $p_i^{\alpha_i}$ și vom nota cu c_i' pe acela dintre $c_1, c_2, \ldots, c_{\varphi(p)}$ care reprezintă clasa de resturi modulo p de ordin δ_i'. Atunci clasa de resturi

modulo p reprezentată de $c_i'^{a_i}$, unde a_i este numărul natural definit prin $\delta_i' = a_i p_i^{\alpha_i}$, are ordinul $p_i^{\alpha_i}$. Deci clasa de resturi modulo p reprezentată de

$$c_1'^{a_1} c_2'^{a_2} \ldots c_r'^{a_r}$$

are ordinul $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r} = \tau$, deoarece $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_r^{\alpha_r}$ sînt prime două cîte două. Din cauză că τ este ordinul unei clase de resturi modulo p avem $\tau \mid \varphi(p)$, deci $\tau \leqslant \varphi(p)$. Pe de altă parte congruența

$$x^\tau \equiv 1 \pmod{p}$$

are ca soluții pe $c_1, c_2, \ldots, c_{\varphi(p)}$, deoarece $c_i^{\delta_i} \equiv 1 \pmod{p}$, $\tau = \delta_i b_i$, deci $c_i^\tau \equiv 1 \pmod{p}$ pentru $i = 1, 2, \ldots, n$. Trebuie să avem $\tau \geqslant \varphi(p)$, deoarece coeficienții polinomului $x^\tau - 1$ nu se divid cu p, iar congruența $x^\tau \equiv 1 \pmod{p}$ are cel puțin $\varphi(p)$ soluții distincte care sînt $c_1, c_2, \ldots, c_{\varphi(p)}$. Deci

$$\tau = \varphi(p)$$

și am dovedit existența rădăcinilor primitive modulo p, unde p este număr prim.

Teoremă. *Există rădăcini primitive modulo $\pm p^\beta$, unde p este număr prim pozitiv diferit de 2, iar β este un număr natural. Dacă g este o rădăcină primitivă modulo p, iar t este un număr întreg astfel încît $(g+pt)^{p-1} = 1 + pu$, unde $p \nmid u$, atunci $g+pt$ este o rădăcină primitivă modulo $\pm p^\beta$.*

Demonstrație. Fie g o rădăcină primitivă modulo p. Vom arăta că există un număr întreg t astfel încît să avem

$$(g+pt)^{p^n(p-1)} = 1 + p^{n+1} u_{n+1},$$

unde $p \nmid u_{n+1}$ pentru orice număr întreg n nenegativ. Să arătăm acest lucru prin inducție completă.

Pentru $n = 0$ putem scrie

$$(g+pt)^{p-1} = g^{p-1} + C_{p-1}^1 g^{p-2} pt + p^2 U = 1 + p(T_0 - g^{p-2} t + pT),$$

unde $g^{p-1} = 1 + pT_0$, conform teoremei lui Fermat, p fiind pozitiv, și $T = U + g^{p-2} t$, deoarece am ținut seama și de $C_{p-1}^1 = p - 1$. Dar

$$T_0 - g^{p-2} t + pT \equiv -g^{p-2} t + T_0 \pmod{p}$$

și atunci cînd t parcurge un sistem complet de resturi modulo p rezultă că $-g^{p-2} t + T_0$ parcurge tot un sistem complet de resturi

modulo p, deoarece $-g^{p-2}$ este prim cu modulul p, g fiind rădăcină primitivă modulo p. Într-un sistem complet de resturi modulo p numai unul din numere este divizibil cu p, ceilalți fiind toți nedivizibili cu p. Putem alege deci pe t astfel ca $p\nmid -g^{p-2}t+T_0$ și atunci $p\nmid T_0-g^{p-2}t+pT$. Punînd $u_1=T_0-g^{p-2}t+pT$ am dovedit proprietatea pentru $n=0$.

Presupunem acum proprietatea dovedită pentru $n=i$. Să o dovedim și pentru $n=i+1$. Avem

$$(g+pt)^{p^i(p-1)}=1+p^{i+1}u_{i+1}.$$

Obținem

$$(g+pt)^{p^{i+1}(p-1)}=(1+p^{i+1}u_{i+1})^p=1+C_p^1p^{i+1}u_{i+1}+$$
$$+C_p^2p^{2(i+1)}u_{i+1}^2+p^{3(i+1)}K=1+p^{i+2}(u_{i+1}+p^{i+1}\frac{p-1}{2}u_{i+1}^2+$$
$$+p^{2i+1}K)=1+p^{i+2}(u_{i+1}+p^{i+1}k).$$

Acest rezultat este corect în cazul cînd p este un număr prim pozitiv diferit de 2 și nu este corect în cazul cînd $p=2$, deoarece pentru $p=2$ avem

$$(1+2^{i+1}u_{i+1})^2=1+2\cdot 2^{i+1}u_{i+1}+2^{2(i+1)}u_{i+1}^2=1+2^{i+2}(u_{i+1}+2^iu_{i+1}^2)$$

și nu putem scrie

$$(1+2^{i+1}u_{i+1})^2=1+2^{i+2}(u_{i+1}+2^{i+1}k),$$

deoarece se presupune că $2\nmid u_{i+1}$.

În cazul cînd p este prim pozitiv și diferit de 2 obținem $p\nmid u_{i+2}$, unde $u_{i+2}=u_{i+1}+p^{i+1}k$, deoarece $p\nmid u_{i+1}$, iar $p\mid p^{i+1}k$ în cazul cînd i este un număr întreg nenegativ. Cu aceasta se încheie demonstrația prin inducție completă a proprietății considerate la începutul demonstrației. Datorită demonstrației prin inducție completă rezultă că e suficient să existe un număr întreg t astfel ca $(g+pt)^{p-1}=1+pu$ cu $p\nmid u$ ca proprietatea de mai sus să fie adevărată.

Să notăm cu δ ordinul clasei de resturi modulo $\pm p^\beta$ reprezentată de $g+pt$. Această clasă de resturi modulo $\pm p^\beta$ este primă cu modulul, deoarece g este prim cu p, iar $g+pt$ face parte din clasa de resturi modulo p reprezentată de g, deci $g+pt$ este prim cu $\pm p^\beta$. Deci

$$\delta\mid p^{\beta-1}(p-1),$$

deoarece $p^{\beta-1}(p-1)=\varphi(\pm p^\beta)$.

Pe de altă parte, din $(g+pt)^\delta\equiv 1 \pmod{\pm p^\beta}$ deducem

$$g^\delta\equiv 1 \pmod p,$$

deci $p-1\mid\delta$, deoarece ordinul clasei de resturi modulo p reprezentată de g este $\varphi(p)=p-1$. Așadar $\delta=(p-1)c$, deci $(p-1)c\mid p^{\beta-1}(p-1)$ deci $c\mid p^{\beta-1}$, deci $c=p^r$ cu $0\leqslant r\leqslant\beta-1$. Deci $\delta=p^r(p-1)$. Dar

$$(g+pt)^{p^r(p-1)}=1+p^{r+1}u_{r+1},$$

unde $p\nmid u_{r+1}$. Avem

$$(g+pt)^\delta\equiv 1 \pmod{\pm p^\beta},$$

deci $1+p^{r+1}u_{r+1}\equiv 1 \pmod{\pm p^\beta}$, deoarece $\delta=p^r(p-1)$. Obținem $p^{r+1}u_{r+1}\equiv 0 \pmod{\pm p^\beta}$, deci $p^\beta\mid p^{r+1}u_{r+1}$. Avînd $p\nmid u_{r+1}$ avem $(u_{r+1},\ p)\cong 1$, deci $(u_{r+1},\ p^\beta)\cong 1$, deci $p^\beta\mid p^{r+1}$, deci $\beta\leqslant r+1$, adică $\beta-1\leqslant r$. Din cauză că am arătat că și $r\leqslant\beta-1$, avem $r=\beta-1$, deci $\delta=p^{\beta-1}(p-1)=\varphi(\pm p^\beta)$ și am dovedit teorema.

Teoremă. *Există rădăcini primitive modulo $\pm 2p^\beta$, unde p este un număr prim pozitiv diferit de 2, iar β este un număr natural. Dacă g este rădăcină primitivă modulo p^β, atunci numărul care este impar dintre g și $g+p^\beta$ este rădăcină primitivă modulo $\pm 2p^\beta$.*

Demonstrație. Dacă g este rădăcină primitivă modulo p^β, atunci

$$g^{\varphi(p^\beta)}\equiv 1 \pmod{p^\beta},$$
$$g^\mu\not\equiv 1 \pmod{p^\beta},$$

pentru orice număr întreg μ pentru care $0<\mu<\varphi(p^\beta)$. Dacă g este impar, avem $2\mid g^{\varphi(p^\beta)}-1$ și $p^\beta\mid g^{\varphi(p^\beta)}-1$, deci $\pm 2p^\beta\mid g^{\varphi(p^\beta)}-1$, deci

$$g^{\varphi(p^\beta)}\equiv 1 \pmod{\pm 2p^\beta}.$$

Acest lucru se poate scrie

$$g^{\varphi(\pm 2p^\beta)}\equiv 1 \pmod{\pm 2p^\beta},$$

deoarece $\varphi(\pm 2p^\beta)=\varphi(p^\beta)$. Apoi dacă $g^\mu\not\equiv 1 \pmod{p^\beta}$, atunci și $g^\mu\not\equiv 1 \pmod{\pm 2p^\beta}$ pentru orice număr întreg μ pentru care $0<\mu<\varphi(\pm 2p^\beta)$. Am demonstrat deci că dacă g este impar și este rădăcină primitivă modulo p^β atunci g este rădăcină primi-

tivă și modulo $\pm 2p^\beta$. Dacă g nu este impar, atunci $g+p^\beta$ este impar și face parte din aceeași clasă de resturi modulo p^β ca și g și raționamentul de mai sus i se aplică lui $g+p^\beta$.

Teoremă. *Există rădăcini primitive modulo 0 și modulo* $\pm 2^\alpha$, *unde* $\alpha=0, 1, 2$. *Numărul* -1 *este rădăcină primitivă modulo 0 și modulo* $\pm 2^\alpha$, *unde* $\alpha=0, 1, 2$.

Demonstrație. Dacă $\alpha=0$, atunci $\pm 2^\alpha=\pm 1$ și $\varphi(\pm 2^\alpha)=1$. Avem

$$(-1)^1 \equiv 1 \pmod{\pm 1},$$

$$(-1)^\mu \not\equiv 1 \pmod{\pm 1},$$

pentru orice număr întreg μ pentru care $0<\mu<1$, deoarece un astfel de μ nu există.

Dacă $\alpha=1$, atunci $\pm 2^\alpha=\pm 2$ și $\varphi(\pm 2)=1$. Avem

$$(-1)^1 \equiv 1 \pmod{\pm 2},$$

$$(-1)^\mu \not\equiv 1 \pmod{\pm 2},$$

pentru orice număr întreg μ pentru care $0<\mu<1$, deoarece un astfel de μ nu există.

Dacă $\alpha=2$, atunci $\pm 2^\alpha=\pm 2^2$ și $\varphi(\pm 2^\alpha)=2$. Avem și $\varphi(0)=2$ deci

$$(-1)^2 \equiv 1 \pmod{\pm 2^2},$$

$$(-1)^\mu \not\equiv 1 \pmod{\pm 2^2},$$

sau

$$(-1)^2 \equiv 1 \pmod{0},$$

$$(-1)^\mu \not\equiv 1 \pmod{0},$$

pentru orice număr întreg μ pentru care $0<\mu<2$, deoarece singura valoare a lui μ este 1, iar

$$(-1)^1 \not\equiv 1 \pmod{\pm 2^2}$$

sau

$$(-1)^1 \not\equiv 1 \pmod{0}.$$

Deci -1 este rădăcină primitivă modulo 0 și modulo $\pm 2^\alpha$, unde $\alpha=0, 1, 2$.

5.4. Determinarea rădăcinilor primitive modulo m

Vom da un procedeu pentru determinarea rădăcinilor primitive modulo m în cazul în care ele există. Acest procedeu este dat de următoarea teoremă.

Teoremă. *Condiția necesară și suficientă ca un număr întreg* g *prim cu* m *să fie rădăcină primitivă modulo* m *este ca* g *să nu satisfacă nici una din congruențele*

$g^{\frac{c}{p_1}} \equiv 1 \pmod m$, $g^{\frac{c}{p_2}} \equiv 1 \pmod m$, ..., $g^{\frac{c}{p_r}} \equiv 1 \pmod m$, *unde* $c=\varphi(m)$, iar $p_1, p_2, \ldots, p_r$ *sînt toți divizorii primi pozitivi ai lui* c *diferiți doi cîte doi.*

Demonstrație. Dacă g este rădăcină primitivă modulo m, atunci congruențele de mai sus nu sînt satisfăcute, deoarece se contrazice definiția rădăcinii primitive modulo m. Reciproc, admitem că g nu satisface nici una din congruențele de mai sus și fie δ ordinul clasei de resturi modulo m, primă cu modulul, pe care o reprezintă g. Dacă $\delta<\varphi(m)$, atunci din faptul că $\delta \mid \varphi(m)$ obținem $\varphi(m)=\delta a$ cu $a>1$, deci există un divizor prim pozitiv p_i al lui $c=\varphi(m)$ astfel încît $p_i \mid a$. În aceste condiții obținem $a=p_i b_i$, deci $\frac{c}{p_i}=\delta b$ este un număr întreg, iar $g^{\frac{c}{p_i}} \equiv (g^\delta)^b \equiv 1 \pmod m$, ceea ce este contradictoriu, deci $\delta=\varphi(m)$ și g este rădăcină primitivă modulo m.

Observație. Este indicat să folosim această teoremă numai în cazul cînd modulul m este prim pozitiv diferit de 2, deoarece cunoscînd o rădăcină primitivă modulo p, unde p este prim pozitiv diferit de 2, putem determina rădăcinile primitive modulo $\pm p^\beta$, $\pm 2p^\beta$, unde β este un număr natural, cu ajutorul teoremelor de existență respective. În cazul modulelor 0, $\pm 2^\alpha$ cu $\alpha=0, 1, 2$ cunoaștem că o rădăcină primitivă modulo $\pm 2^\alpha$ și modulo 0 este -1, iar în cazul celorlalte module m știm că nu există rădăcini primitive modulo m, lucru pe care teorema pentru determinarea rădăcinilor primitive modulo m trebuie să ne-o confirme, dar numai în urma unor calcule numeroase și obositoare pe care nu merită să le mai facem, tocmai pentru că știm

că nu există rădăcini primitive pentru modulele $m \neq 0$, $m \neq \pm 2^\alpha$, $m \neq \pm p^\beta$, $m \neq \pm 2p^\beta$, unde $\alpha = 0, 1, 2$, iar p este număr prim pozitiv diferit de 2 și β este un număr natural.

Exemplul 1. Să determinăm o rădăcină primitivă modulo $p = 41$.

Avem $c = \varphi(41) = 40 = 2^3 5$. Deci $p_1 = 2$, $p_2 = 5$. Orice număr întreg g prim cu 41 care nu satisface nici una din congruențele

$$g^{20} \equiv 1 \pmod{41}, \quad g^8 \equiv 1 \pmod{41}$$

este rădăcină primitivă modulo 41, iar numerele întregi g care satisfac cel puțin una din aceste congruențe nu sînt rădăcini primitive modulo 41.

Pentru a determina o rădăcină primitivă modulo 41 trebuie deci să considerăm, mai întîi, un sistem redus de resturi modulo 41, deoarece există clase de resturi modulo 41, prime cu 41, de ordin $\varphi(41)$, iar reprezentanții lor se află printre elementele unui sistem redus de resturi modulo 41, ordinul unei clase de resturi modulo m, primă cu modulul, nedepinzînd de reprezentantul clasei.

Numerele întregi de la 1 la 40 formează un sistem redus de resturi modulo m. Numărul 1 nu este rădăcină primitivă modulo 41, deoarece satisface ambele congruențe de mai sus.

Să încercăm cu 2. Avem $2^5 = 32$, deci $2^5 \equiv 32 - 41 \equiv -9 \pmod{41}$, $2^{10} \equiv 9^2 \equiv 81 \equiv -1 \pmod{41}$, $2^{20} \equiv 1 \pmod{41}$. Deci 2 nu este rădăcină primitivă modulo 41.

Să încercăm cu 3. Avem $3^2 \equiv 9 \pmod{41}$, $3^4 \equiv 9^2 \equiv 81 \equiv -1 \pmod{41}$, deci $3^8 \equiv 1 \pmod{41}$, deci 3 nu este rădăcină primitivă modulo 41.

Să încercăm cu 4. Avem $2^{20} \equiv 1 \pmod{41}$, deci $4^{20} \equiv 1 \pmod{41}$, deci 4 nu este rădăcină primitivă modulo 41.

Să încercăm cu 5. Avem $5^2 \equiv 25 \equiv -16 \pmod{41}$, deci $5^2 \equiv -2^4 \pmod{41}$, deci $5^{10} \equiv -2^{20} \equiv -1 \pmod{41}$, deci $5^{20} \equiv 1 \pmod{41}$, deci 5 nu este rădăcină primitivă modulo 41.

Să încercăm cu 6. Avem $6^2 \equiv 36 \equiv -5 \pmod{41}$, $6^4 \equiv 25 \equiv -16 \equiv -2^4 \pmod{41}$, $6^8 \equiv 2^8 \equiv 2^5 2^3 \equiv -9 \cdot 8 \equiv -72 \equiv 10 \pmod{41}$ și $6^{20} \equiv -2^{20} \equiv -1 \pmod{41}$. Deci 6 este rădăcină primitivă modulo 41.

Exemplul 2. Să determinăm o rădăcină primitivă modulo $m = 41^2$. Trebuie să determinăm un număr întreg t astfel încît să avem

$$(6 + 41t)^{40} = 1 + 41u, \quad 41 \nmid u.$$

Deoarece $(6+41t)^{40} = 6^{40} + C_{40}^1 6^{39} 41t + 41^2 U = 6^{40} + (41-1)6^{39}41t + 41^2 U = 6^{40} - 6^{39}41t + 41^2(6^{39}t + U)$, vom calcula pe 6^{40} modulo 41^2. Vom avea $6^{40} = 1 + 41T_0 = 1 + 41(r + 41k) = 1 + 41r + 41^2 k$, unde $6^{40} = 1 + 41T_0$ este conform teoremei lui Fermat, și deci

$$(6 + 41t)^{40} = 1 + 41(r - 6^{39}t + 41(k + 6^{39}t + U)).$$

În aceste relații $0 \leqslant r < 41$. Dacă $r = 0$ luăm pentru t orice număr întreg care nu se divide cu 41, în particular luăm $t = 1$. Dacă însă $r \neq 0$, atunci putem lua $t = 0$. În ambele cazuri alegerea lui t duce la aceea că paranteza $(r - 6^{39}t + 41(k + 6^{39}t + U))$ nu se divide cu 41.

Determinarea lui r din congruența

$$6^{40} \equiv 1 + 4r \pmod{41^2}$$

se face în felul următor. Avem $41^2 = 1681$. Apoi

$$6^{40} = (6^4)^{10} = (36^2)^{10} = (1296)^{10}.$$

Deci

$$6^{40} \equiv (1296 - 1681)^{10} \equiv 385^{10} \equiv (385^2)^5 \equiv 148225^5 \equiv 297^5 \pmod{41^2}.$$

Mai departe

$$6^{40} \equiv 297^5 \equiv ((297)^2)^2 297 \equiv (88209)^2 297 \equiv 797^2 297 \pmod{41^2}.$$

Deci

$$6^{40} \equiv (797 \cdot 297)797 \equiv 236709 \cdot 797 \equiv 1369 \cdot 797 \pmod{41^2}.$$

Așadar

$$6^{40} \equiv (1369 - 1681)797 \equiv -312 \cdot 797 \equiv -248664 \equiv -1557 \pmod{41^2}$$

Deci

$$6^{40} \equiv -1557 + 1681 \equiv 124 \equiv 1 + 41 \cdot 3 \pmod{41^2}.$$

Deoarece $r = 3$ luăm $t = 0$ și atunci

$$6^{40} = 1 + 41(3 + 41k)$$

cu $41 \nmid 3 + 41k$. Deci 6 este rădăcină primitivă modulo 41^2.

Exemplul 3. Să determinăm o rădăcină primitivă modulo $2 \cdot 41^2$.

Dintre 6 și $6 + 41^2 = 6 + 1681 = 1687$, numărul 1687 este impar, deci 1687 este rădăcină primitivă modulo $2 \cdot 41^2$.

5.5. Rădăcini primitive în corpul numerelor complexe pentru ecuația binomă

Dacă sistemul de relații

$$a^{\varphi(m)} \equiv 1 \pmod{m},$$

$$a^{\mu} \not\equiv 1 \pmod{m},$$

oricare ar fi numărul întreg μ astfel încît $0<\mu<\varphi(m)$, prin care se definește o rădăcină primitivă modulo m, îl transcriem cu ajutorul claselor de resturi modulo m, obținem o formulare echivalentă sub forma

$$C_a^{\varphi(m)} = C_1,$$

$$C_a^{\mu} \neq C_1$$

oricare ar fi numărul întreg μ astfel încît $0<\mu<\varphi(m)$.

În noua formulare, putem spune că în inelul claselor de resturi modulo m o clasă de resturi C_a modulo m primă cu modulul este o rădăcină primitivă modulo m dacă C_a este o rădăcină a ecuației binome $x^{\varphi(m)}=C_1$ astfel încît $C_a^{\mu}\neq C_1$ oricare ar fi numărul întreg μ pentru care $0<\mu<\varphi(m)$.

Într-o formulare analoagă, putem spune că în inelul claselor de resturi modulo m o clasă de resturi C_a modulo m primă cu modulul este de ordin δ, unde δ este un număr natural, dacă C_a este o rădăcină a ecuației binome $x^{\delta}=C_1$ astfel încît $C_a^{\mu}\neq C_1$ oricare ar fi numărul întreg μ pentru care $0<\mu<\delta$.

Datorită celor spuse mai sus, sîntem îndrumați să dăm următoarea definiție.

Definiție. *Se numește rădăcină primitivă a ecuației*

$$x^n = 1,$$

unde n este un număr natural, o rădăcină ρ a acestei ecuații astfel încît

$$\rho^s \neq 1$$

oricare ar fi numărul întreg s pentru care $0<s<n$.

Teoremă. *Există rădăcini primitive ale ecuației*

$$x^n = 1.$$

Demonstrație. Luăm $\rho = e^{\frac{2\pi i}{n}}$, unde e este baza logaritmilor naturali, iar i este una dintre rădăcinile ecuației $x^2+1=0$. Numărul ρ luat este o rădăcină primitivă a ecuației $x^n=1$. Într-adevăr, mai întîi, $\rho = e^{\frac{2\pi i}{n}}$ este o rădăcină a ecuației $x^n=1$, deoarece

$$\rho^n = \left(e^{\frac{2\pi i}{n}}\right)^n = e^{2\pi i} = \cos 2\pi + i \sin 2\pi = 1 + i\cdot 0 = 1.$$

Apoi pentru orice număr întreg s pentru care $0<s<n$ avem $\rho^s \neq 1$. Într-adevăr, dacă am avea $\rho^s=1$, deoarece $\rho^s = \left(e^{\frac{2\pi i}{n}}\right)^s = e^{\frac{2\pi s i}{n}} = \cos\frac{2\pi s}{n} + i \sin\frac{2\pi s}{n}$, am avea $\cos\frac{2\pi s}{n}=1$ și $\sin\frac{2\pi s}{n}=0$. Din $\sin\frac{2\pi s}{n}=0$ rezultă $\frac{2\pi s}{n}=k\pi$, unde k este un număr întreg. Deci $2s=nk$. Ținînd seama și de $0<s<n$, obținem $0<sk<nk$, deoarece $k>0$, ceea ce rezultă din $2s=nk$ și $0<s<n$. Deci $0<sk<2s$, deci $0<k<2$, deoarece $0<s$, deci $k=1$. Dar atunci $\cos\frac{2\pi s}{n}=\cos\pi=-1$ contrar lui $\cos\frac{2\pi s}{n}=1$. Am arătat deci că $\rho = e^{\frac{2\pi i}{n}}$ este o rădăcină primitivă a ecuației binome $x^n=1$.

Teoremă. *Dacă ρ este o rădăcină primitivă a ecuației*

$$x^n = 1,$$

unde n este un număr natural, atunci $\rho^0, \rho^1, \ldots, \rho^{n-1}$ reprezintă toate rădăcinile ecuației $x^n=1$.

Demonstrație. Avem $\rho^i \neq \rho^j$ cu $i\neq j$ și $i, j=0, 1, \ldots, n-1$, deoarece dacă $\rho^i=\rho^j$ și $i\neq j$, $i, j=0, 1, \ldots, n-1$, considerînd că $i>j$ obținem $\rho^{i-j}=1$, ceea ce contrazice faptul că ρ este rădăcină primitivă a ecuației considerate, deoarece din $i, j=0,1,\ldots,n-1$ și $i>j$ rezultă $0<i-j<n$. Deci numerele $\rho^0, \rho^1, \ldots, \rho^{n-1}$ sînt distincte și fiind în număr de n cît este gradul ecuației $x^n=1$, rezultă că teorema este demonstrată, numerele ρ^i, $i=0, 1, \ldots, n-1$ fiind rădăcini ale ecuației $x^n=1$, deoarece $(\rho^i)^n = (\rho^n)^i = 1$.

Capitolul 6

INDICI MODULO m

6.1. Indici modulo $\pm p^\beta$ și $\pm 2p^\beta$ unde p este prim pozitiv impar, iar β este număr natural

Să notăm cu m oricare dintre numerele $\pm p^\beta$ și $\pm 2p^\beta$, să punem $c=\varphi(m)$ și fie g o rădăcină primitivă modulo m.

Noțiunea de indice în raport cu modulul m considerat mai sus este inspirată de următoarea teoremă.

Teoremă. *Dacă γ parcurge un sistem complet de resturi modulo c atunci g^γ parcurge un sistem redus de resturi modulo m.*

Demonstrație. Dacă notăm cu $\gamma_1, \gamma_2, \ldots, \gamma_c$ un sistem complet de resturi modulo c atunci se constată că:

(1) numărul numerelor întregi g^{γ_i} pentru $i=1, 2, \ldots, c$ este egal cu $\varphi(m)$, deoarece $c=\varphi(m)$;

(2) $m \nmid g^{\gamma_i}-g^{\gamma_j}$, unde $i \neq j$, $i, j=1, 2, \ldots, c$, deoarece din $m \mid g^{\gamma_i}-g^{\gamma_j}$ obținem $g^{\gamma_i} \equiv g^{\gamma_j} \pmod m$, deci $\gamma_i \equiv \gamma_j \pmod c$, c fiind ordinul clasei de resturi modulo m, primă cu modulul, iar $\gamma_i \equiv \gamma_j \pmod c$ contrazice faptul că γ_i, γ_j, $i \neq j$, $i, j=1, 2, \ldots, c$, fac parte din același sistem complet de resturi modulo m;

(3) $(g^{\gamma_i}, m) \cong 1$, pentru $i=1, 2, \ldots, c$, deoarece $(g, m) \cong 1$, g fiind rădăcină primitivă modulo m.

Cu aceasta teorema este demonstrată.

Definiție. *Dacă a este un număr întreg prim cu m, iar g este o rădăcină primitivă modulo m, indice al lui a modulo m în raport cu baza g este un număr întreg γ astfel încît*

$$a \equiv g^\gamma \pmod m.$$

Se scrie $\gamma=\operatorname{ind}_g a$ sau mai scurt $\gamma=\operatorname{ind} a$.

Observație. Există ind a *oricare ar fi numărul întreg a prim cu m,* deoarece clasa de resturi modulo m primă cu modulul reprezentată de a este reprezentată conform teoremei precedente și de un număr întreg de forma g^γ, unde g este o rădăcină primitivă modulo m, iar γ este un număr întreg.

Indicele lui a modulo m în raport cu baza g este unic în sensul că dacă γ' și γ sînt valori ale indicelui lui a modulo m în raport cu baza g, atunci

$$\gamma' \equiv \gamma \pmod c.$$

Într-adevăr, din $a \equiv g^{\gamma'} \pmod m$ și $a \equiv g^\gamma \pmod m$ rezultă $g^{\gamma'} \equiv g^\gamma \pmod m$ deci $\gamma' \equiv \gamma \pmod c$, c fiind ordinul clasei de resturi modulo m primă cu modulul reprezentată de g.

În cazul cînd luăm un anumit sistem complet de resturi modulo c, cum ar fi $0, 1, \ldots, c-1$ sau $1, 2, \ldots, c$, atunci valoarea indicelui lui a modulo m în raport cu baza g este un singur număr întreg din acest sistem complet de resturi modulo c, conform teoremei precedente.

Proprietăți ale indicelui modulo m.

(1) *Numerele întregi dintr-o clasă de resturi modulo m, primă cu modulul, au un același indice modulo m în raport cu baza g și numai ele au un indice dat.*

Într-adevăr, dacă $\gamma=\operatorname{ind}_g a$, iar $b \equiv a \pmod m$, atunci din $a \equiv g^\gamma \pmod m$ rezultă și $b \equiv g^\gamma \pmod m$. Reciproc dacă $a \equiv g^\gamma \pmod m$ și $b \equiv g^\gamma \pmod m$ atunci $a \equiv b \pmod m$. Mai trebuie adăugat că fiind dat un număr întreg γ există totdeauna un număr întreg a prim cu m astfel încît $a \equiv g^\gamma \pmod m$.

Această proprietate ne arată că noțiunea de indice se asociază claselor de resturi modulo m prime cu modulul, iar nu fiecărui număr întreg în parte.

(2) *Dacă* γ_a *este indice al lui* a *modulo* m *în raport cu baza* g, *iar* γ_b *este indice al lui* b *modulo* m *în raport cu baza* g, *atunci* $\gamma_a+\gamma_b$ *este indice al lui* ab *modulo* m *în raport cu baza* g.

Într-adevăr, dacă $a\equiv g^{\gamma_a} \pmod m$, iar $b\equiv g^{\gamma_b} \pmod m$, atunci $ab\equiv g^{\gamma_a+\gamma_b} \pmod m$.

În particular $\operatorname{ind} a^n \equiv n \operatorname{ind} a \pmod c$.

Această proprietate ne arată că indicele modulo m are proprietăți analoage cu cele ale logaritmului. În favoarea acestei aprecieri mai intervine și faptul că

$$\operatorname{ind}_{g_2} a \equiv (\operatorname{ind}_{g_1} a)\ (\operatorname{ind}_{g_2} g_1) \pmod c,$$

unde g_1 *și* g_2 *sînt două rădăcini primitive modulo* m.

Într-adevăr, din $a\equiv g_1^{\gamma_1} \pmod m$ și $g_1\equiv g_2^{\gamma_2} \pmod m$, unde $\gamma_1=\operatorname{ind}_{g_1} a$, $\gamma_2=\operatorname{ind}_{g_2} g_1$ rezultă $a\equiv g_1^{\gamma_1}\equiv (g_2^{\gamma_2})^{\gamma_1}\equiv g_2^{\gamma_1\gamma_2} \pmod m$, deci $\operatorname{ind}_{g_2} a\equiv(\operatorname{ind}_{g_1} a)\ (\operatorname{ind}_{g_2} g_1) \pmod c$, ceea ce reprezintă regula de schimbare a bazei în raport cu care se ia indicele modulo m, această schimbare de bază fiind analoagă cu cea de la logaritm.

(3) *Avem*

$$(\operatorname{ind} a,\ c)\cong \frac{c}{\delta},$$

unde δ *este ordinul clasei de resturi modulo* m, *primă cu modulul, reprezentată de* a.

Într-adevăr, conform definiției celui mai mare divizor comun a două numere întregi avem de dovedit că

1) $\dfrac{c}{\delta} \Big| \operatorname{ind} a, \dfrac{c}{\delta} \Big| c$,

2) pentru orice număr întreg Δ pentru care $\Delta|\operatorname{ind} a$, $\Delta|c$ rezultă $\Delta \Big| \dfrac{c}{\delta}$.

Relațiile $\dfrac{c}{\delta} \Big| \operatorname{ind} a, \dfrac{c}{\delta} \Big| c$ se obțin în felul următor. Luăm una din relațiile care intervin în definiția ordinului clasei de resturi modulo m primă cu modulul reprezentată de a, anume luăm relația

$$a^\delta \equiv 1 \pmod m.$$

Avem $a\equiv g^{\operatorname{ind} a} \pmod m$, unde g este o rădăcină primitivă modulo m, deci $g^{\delta \operatorname{ind} a}\equiv 1 \pmod m$, deci $\delta \operatorname{ind} a\equiv 0 \pmod c$,

deoarece c este ordinul clasei de resturi modulo m primă cu modulul reprezentată de g. Apoi avem $\delta|c$, deoarece ordinul δ al clasei de resturi modulo m primă cu modulul reprezentată de a divide indicatorul lui Euler al lui m, adică divide pe c. Așadar $\dfrac{c}{\delta}$ este un număr întreg, care este și diferit de zero, deoarece $c>0$ avînd $c=\varphi(m)$. Atunci din $\delta \operatorname{ind} a\equiv 0 \pmod c$ obținem $\operatorname{ind} a\equiv 0 \left(\bmod \dfrac{c}{\delta}\right)$, deci $\dfrac{c}{\delta} \Big| \operatorname{ind} a$. Pentru a dovedi acum că $\dfrac{c}{\delta} \Big| c$ pornim de la $c|c$ deci $c|c\,\delta$, deci $\dfrac{c}{\delta} \Big| c$, deoarece $\delta\neq 0$, fiind ordin al clasei de resturi modulo m primă cu modulul reprezentată de a, deci $\delta>0$, iar $\delta|c$.

Relația $\Delta \Big| \dfrac{c}{\delta}$ atunci cînd $\Delta|\operatorname{ind} a$, $\Delta|c$ se obține în felul următor. Din $\Delta|\operatorname{ind} a$ rezultă $\operatorname{ind} a\equiv 0 \pmod \Delta$, deci $\dfrac{c}{\Delta} \operatorname{ind} a\equiv 0 \left(\bmod \dfrac{c}{\Delta}\Delta\right)$, deoarece $\dfrac{c}{\Delta}$ este un număr întreg, avînd $\Delta|c$, deci $\dfrac{c}{\Delta} \operatorname{ind} a\equiv 0 \pmod c$, deci $g^{\frac{c}{\Delta} \operatorname{ind} a}\equiv 1 \pmod m$, deoarece c este ordinul clasei de resturi modulo m primă cu modulul, reprezentată de g. Am obținut deci $a^{\frac{c}{\Delta}}\equiv 1 \pmod m$, deoarece $a\equiv g^{\operatorname{ind} a} \pmod m$. Din $a^{\frac{c}{\Delta}}\equiv 1 \pmod m$ obținem $\delta \Big| \dfrac{c}{\Delta}$, deoarece δ este ordinul clasei de resturi modulo m primă cu modulul reprezentată de a. Din $\delta \Big| \dfrac{c}{\Delta}$ obținem $\delta\Delta|c$ și apoi $\Delta \Big| \dfrac{c}{\delta}$, deoarece $\delta|c$ și $\delta\neq 0$ cum am arătat mai sus.

În felul acesta proprietatea considerată este demonstrată. Această proprietate justifică suprimarea bazei g în notația indicelui lui a modulo m, deoarece cel mai mare divizor comun al lui $\operatorname{ind} a$ și c nu depinde de alegerea bazei g.

Datorită utilității lor, indicii modulo p, unde p este prim, se calculează și se tabulează. Acest lucru se face cu ajutorul unei rădăcini primitive modulo p.

De exemplu, pentru $p=41$ luăm $g=6$. Apoi facem următoarele calcule :

$6^0 \equiv 1 \pmod{41}$,
$6^1 \equiv 6 \pmod{41}$,
$6^2 \equiv 36 \pmod{41}$,
$6^3 \equiv 36 \cdot 6 \equiv -5 \cdot 6 \equiv -30 \equiv 11 \pmod{41}$,
$6^4 \equiv 11 \cdot 6 \equiv 66 \equiv 25 \pmod{41}$,
$6^5 \equiv 25 \cdot 6 \equiv -16 \cdot 6 \equiv -96 \equiv -14 \equiv 27 \pmod{41}$,
$6^6 \equiv 27 \cdot 6 \equiv -14 \cdot 6 \equiv -84 \equiv -2 \equiv 39 \pmod{41}$,
$6^7 \equiv 39 \cdot 6 \equiv -2 \cdot 6 \equiv -12 \equiv 29 \pmod{41}$,
$6^8 \equiv 29 \cdot 6 \equiv -12 \cdot 6 \equiv -72 \equiv 10 \pmod{41}$,
$6^9 \equiv 10 \cdot 6 \equiv 60 \equiv 19 \pmod{41}$,
$6^{10} \equiv 19 \cdot 6 \equiv 114 \equiv 32 \pmod{41}$,
$6^{11} \equiv 32 \cdot 6 \equiv -9 \cdot 6 \equiv -54 \equiv -13 \equiv 28 \pmod{41}$

și așa mai departe pînă la puterea 39-*a* a lui 6, deoarece numerele de la 0 la 39 formează un sistem complet de resturi modulo $40 = \varphi(41)$ și deci puterile lui 6 de la 6^0 la 6^{39} formează un sistem redus de resturi modulo 41.

Dacă notăm cu N numerele 1, 6, 36, 11, 25, 27, 39, 29, 10, 19, 32, 28, ... care fac parte din sistemul redus de resturi modulo 41 format din numerele naturale prime cu 41 și mai mici ca 41 și dacă notăm cu I numerele 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, ... care fac parte din sistemul complet de resturi modulo $40 = \varphi(41)$ format din numerele de la 0 la 39 putem alcătui următoarele două tabele :

Tabela indicilor

N	0	1	2	3	4	5	6	7	8	9
0		0	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9
2	34	14	29	36	13	4	17	5	11	7
3	23	28	10	18	19	21	2	32	35	6
4	20									

Tabela numerelor

I	0	1	2	3	4	5	6	7	8	9
0	1	6	36	11	25	27	39	29	10	19
1	32	28	4	24	21	3	18	26	33	34
2	40	35	5	30	16	14	2	12	31	22
3	9	13	37	17	20	38	23	15	8	7

Numerele N și I în acest exemplu sînt formate din cel mult două cifre zecimale. În aceste tabele, coloana de numere de pe verticala dedesubtul lui N și a lui I cuprinde cifrele zecilor din

numerele N și I respectiv, iar șirul de numere de pe orizontală de la dreapta lui N și a lui I cuprinde cifrele unităților din numerele N respectiv I. Valoarea indicelui I pentru un număr N este înscrisă în tabela indicilor la intersecția liniei orizontale care trece prin cifra zecilor lui N cu linia verticală care trece prin cifra unităților lui N. Valoarea lui N pentru un indice I este înscrisă în tabela numerelor la intersecția liniei orizontale care trece prin cifra zecilor lui I cu linia verticală care trece prin cifra unităților lui I.

6.2. Consecințe ale definiției indicilor modulo m

Considerăm că m este oricare dintre numerele $\pm p^\beta$ și $\pm 2p^\beta$ unde p este prim pozitiv impar, iar β este un număr natural și punem $c = \varphi(m)$.

Teoremă. *Condiția necesară și suficientă ca un număr întreg a prim cu m să fie rădăcină primitivă modulo m este ca*

$$(\text{ind } a,\ c) \cong 1.$$

Demonstrație. Dacă a este rădăcină primitivă modulo m, atunci ordinul clasei de resturi modulo m primă cu modulul reprezentată de a este $\delta = c$ și deci din $(\text{ind } a,\ c) \cong \frac{c}{\delta}$ obținem $(\text{ind } a,\ c) \cong 1$. Reciproc, dacă $(\text{ind } a,\ c) \cong 1$, iar δ este ordinul clasei de resturi modulo m primă cu modulul reprezentată de a, atunci $\frac{c}{\delta} = 1$, deoarece $(\text{ind } a,\ c) \cong \frac{c}{\delta}$, deci $\delta = c$ și deci a este rădăcină primitivă modulo m.

Observație. De aici rezultă și un mod de a determina toate rădăcinile primitive modulo m atunci cînd se cunoaște o rădăcină primitivă modulo m. În adevăr, dacă g este o rădăcină primitivă modulo m atunci orice număr întreg a care verifică relația

$$a \equiv g^\gamma \pmod{m},$$

unde $(\gamma, c)\cong 1$, este o rădăcină primitivă modulo m, iar alte rădăcini primitive modulo m nu mai există, deoarece $\gamma=\text{ind } a$ și avem $(\gamma, c)\cong 1$ conform teoremei precedente.

Teoremă. *Într-un sistem redus de resturi modulo m, numărul numerelor care reprezintă clase de resturi modulo m prime cu m de ordin δ este egal cu $\varphi(\delta)$. În particular, numărul rădăcinilor primitive modulo m, este egal cu $\varphi(c)$.*

Demonstrație. Un număr întreg a, dintr-un sistem redus de resturi modulo m, reprezintă o clasă de resturi modulo m primă cu modulul de ordin δ dacă și numai dacă

$$(\text{ind } a, c)\cong \frac{c}{\delta},$$

deci dacă și numai dacă există un număr întreg y astfel încît $\text{ind } a=\frac{c}{\delta}y$ și $(y, \delta)\cong 1$, deoarece din $(\text{ind } a, c)\cong\frac{c}{\delta}$ se deduce $\frac{c}{\delta}\mid \text{ind } a$, deci se deduce existența unui număr întreg y astfel încît $\text{ind } a=\frac{c}{\delta}y$. Dar atunci $(\text{ind } a, c)\cong\frac{c}{\delta}$ este echivalentă cu $\left(\frac{c}{\delta}y, c\right)\cong\frac{c}{\delta}$ sau cu $(y, \delta)\cong 1$, deoarece $\frac{c}{\delta}\neq 0$.

Atunci cînd a parcurge un sistem redus de resturi modulo m putem face ca $\text{ind } a$ să parcurgă sistemul de numere $1, 2, \ldots, c$ care este un sistem complet de resturi modulo $c=\varphi(m)$, la fiecare a corespunzînd un singur număr din sistemul $1, 2, \ldots, c$, fiecare număr din acest sistem corespunzînd cel puțin unui a din sistemul redus de resturi modulo m considerat, conform unicității indicelui modulo m și faptului că într-un sistem redus de resturi modulo m există $c=\varphi(m)$ numere ca și în sistemul $1, 2, \ldots, c$.

Deci pentru a demonstra teorema trebuie să numărăm acel numere dintre $1, 2, \ldots, c$ care se scriu sub forma $\frac{c}{\delta}y$ cu $(y, \delta)\cong 1$.

Dar numerele de forma $\frac{c}{\delta}\ y$ din $1, 2, \ldots, c$ sînt

$$\frac{c}{\delta}\cdot 1, \frac{c}{\delta}\cdot 2, \ldots, \frac{c}{\delta}\delta.$$

Deci y parcurge acele numere din $1, 2, \ldots, \delta$ care sînt prime cu δ. Totalitatea numerelor parcurse de y formează un sistem

redus de resturi modulo δ, deoarece $1, 2, \ldots, \delta$ formează un sistem complet de resturi modulo δ. Deci numărul valorilor lui y este egal cu $\varphi(\delta)$ și cu aceasta teorema este demonstrată.

Exemplu. Într-un sistem redus de resturi modulo 41 numerele care reprezintă clase de resturi modulo 41 prime cu 41 de ordin egal cu 10 sînt acele numere a care îndeplinesc condiția $(\text{ind } a, 40)\cong\frac{40}{10}\cong 4$, deci în sistemul redus de resturi format din numere naturale mai mici ca 41, numerele care reprezintă clase de resturi modulo 41 prime cu 41 de ordin egal cu 10 sînt numerele

$$4, 23, 25, 31,$$

deoarece $\text{ind } 4=12$, $\text{ind } 23=36$, $\text{ind } 25=4$, $\text{ind } 31=28$, conform tabelei de numere alcătuite pentru modulul 41 avînd ca bază a indicilor pe 6. Numărul numerelor 4, 23, 25, 31 este egal cu $\varphi(10)=4$.

În același sistem redus de resturi modulo 41, rădăcinile primitive modulo 41 sînt acele numere a prime cu modulul 41 care îndeplinesc condiția

$$(\text{ind } a, 40)\cong 1$$

și ele sînt 6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35. Numărul acestor numere este egal cu $\varphi(40)=16$.

6.3. Rezolvarea congruenței $x^n\equiv a \pmod m$ cu ajutorul indicilor

Teoremă. *Congruența*

$$x^n\equiv a \pmod m$$

are soluții dacă și numai dacă $d\mid \text{ind } a$, unde $d\cong(n, c)$. În cazul cînd această congruență are soluții, numărul soluțiilor distincte ale acestei congruențe este egal cu d, d fiind considerat pozitiv.

Demonstrație. Să arătăm că congruența

$$x^n\equiv a \pmod m$$

este echivalentă cu congruența

$$n \text{ ind } x \equiv \text{ind } a \pmod{c}.$$

Acest lucru se arată în felul următor. Se consideră o rădăcină primitivă g modulo m. În cazul cînd congruența $x^n \equiv a \pmod{m}$ are soluții, atunci din $(a, m) \cong 1$ rezultă $(x^n, m) \cong 1$ deci $(x, m) \cong 1$. Deci putem scrie $a \equiv g^{\text{ind } a} \pmod{m}$, $x \equiv g^{\text{ind } x} \pmod{m}$ și atunci congruența $x^n \equiv a \pmod{m}$ este echivalentă cu congruența $g^{n \text{ ind } x} \equiv g^{\text{ind } a} \pmod{m}$, care este echivalentă cu congruența

$$n \text{ ind } x \equiv \text{ind } a \pmod{c}.$$

Această ultimă congruență are însă soluții dacă și numai dacă $d \mid \text{ind } a$. Putem considera pe d pozitiv, deoarece există o valoare pozitivă a celui mai mare divizor comun al lui n și c. Atunci numărul soluțiilor distincte ale congruenței considerate este egal cu d în cazul cînd congruența $x^n \equiv a \pmod{m}$ are soluții, deoarece congruența $n \text{ ind } x \equiv \text{ind } a \pmod{c}$, necunoscuta fiind $\text{ind } x$, are în acest caz d soluții distincte.

Exemplul 1. Să considerăm congruența $x^8 \equiv 11 \pmod{41}$. Aici modulul 41 este prim, iar 11 este prim cu 41. Avem $c = \varphi(41) = 40$. Apoi $(8, 40) \cong 8$, $\text{ind}_6 11 = 3$, deci $8 \nmid 3$. Această congruență nu are soluții.

Exemplul 2. Să considerăm congruența $x^{12} \equiv 25 \pmod{41}$. Aici modulul 41 este prim, iar 25 este prim cu 41. Avem $c = \varphi(41) = 40$. Apoi $(12, 40) \cong 4$, $\text{ind}_6 25 = 4$. Deoarece $4 \mid 4$, congruența considerată are soluții. Soluțiile le vom găsi rezolvînd congruența

$$12 \text{ ind}_6 x \equiv \text{ind}_6 25 \pmod{40},$$

adică congruența $12 \text{ ind}_6 x \equiv 4 \pmod{40}$ sau $3 \text{ ind}_6 x \equiv 1 \pmod{10}$. Avem $3 \cdot 3 \equiv -1 \pmod{10}$, deci $3 \cdot 3 \text{ ind}_6 x \equiv 3 \pmod{10}$ sau $\text{ind}_6 x \equiv -3 \pmod{10}$ sau $\text{ind}_6 x \equiv 7 \pmod{10}$. Deci $\text{ind}_6 x \equiv 7 \pmod{40}$, $\text{ind}_6 x \equiv 17 \pmod{40}$, $\text{ind}_6 x \equiv 27 \pmod{40}$, $\text{ind}_6 x \equiv 37 \pmod{40}$.

Consultînd tabela de numere modulo 41, alcătuită în raport cu rădăcina primitivă 6 modulo 41, obținem următoarele soluții distincte ale congruenței considerate, anume $x \equiv 29 \pmod{41}$, $x \equiv 26 \pmod{41}$, $x \equiv 12 \pmod{41}$, $x \equiv 15 \pmod{41}$. Se poate verifica că 29 este o soluție a congruenței considerate, verificarea făcîndu-se în felul următor:

$$29^{12} \equiv (-12)^{12} \equiv 4^{12} 3^{12} \equiv 2^{24} 9^6 \equiv 2^{24} (-32)^6 \equiv 2^{54} (2^5)^6 \equiv 2^{54} \equiv 2^{14} \equiv$$
$$\equiv 2^{10} 2^4 \equiv -2^4 \equiv -16 \equiv 25 \pmod{41}.$$

Am folosit în acest calcul faptul că $2^{10} \equiv -1 \pmod{41}$ lucru pe care l-am stabilit cu ocazia determinării unei rădăcini primitive modulo 41.

Definiție. *Numerele întregi a prime cu m, m fiind un număr întreg oarecare pentru care congruența*

$$x^n \equiv a \pmod{m}$$

are soluții, se numesc resturi de gradul n modulo m, iar cele pentru care congruența de mai sus nu are soluții se numesc neresturi de gradul n modulo m.

Pentru valori particulare ale lui n avem denumiri speciale. Astfel dacă $n = 2$ se vorbește de *resturi pătratice* și *neresturi pătratice*. Dacă $n = 3$ se vorbește de *resturi cubice* și *neresturi cubice*. Dacă $n = 4$ se vorbește de *resturi bipătratice* și *neresturi bipătratice*. Aceste denumiri speciale au apărut din cauză că aceste cazuri particulare au fost studiate mai amănunțit.

Considerînd că m este oricare din numerele $\pm p^\beta$ și $\pm 2p^\beta$ unde p este număr prim impar, iar β este un număr natural avem următoarele teoreme:

Teoremă. *Într-un sistem redus de resturi modulo m avem numai $\frac{c}{d}$ resturi de gradul n modulo m, unde $c = \varphi(m)$, $d \cong (n, c)$ și $d > 0$.*

Demonstrație. Un număr întreg a dintr-un sistem redus de resturi modulo m este rest de gradul n modulo m dacă și numai dacă $d \mid \text{ind } a$.

Atunci cînd a parcurge un sistem redus de resturi modulo m putem face ca $\text{ind } a$ să parcurgă sistemul de numere $1, 2, \ldots, c$ care este un sistem complet de resturi modulo $c = \varphi(m)$, la fiecare a corespunzînd un singur număr dintre $1, 2, \ldots, c$, fiecare număr din acest sistem corespunzînd cel puțin unui a din sistemul redus de resturi modulo m considerat, conform unicității indicelui modulo m și faptului că într-un sistem redus de resturi modulo m există $c = \varphi(m)$ numere ca și în sistemul $1, 2, \ldots, c$.

Deci pentru a demonstra teorema trebuie să numărăm acele numere din $1, 2, \ldots, c$ care se divid cu d. Aceste numere sînt

$$1 \cdot d, \; 2 \cdot d, \ldots, \frac{c}{d} \, d,$$

iar numărul lor este $\frac{c}{d}$ și cu aceasta teorema este demonstrată.

Teoremă. *Un număr întreg a prim cu m este rest de gradul n modulo m dacă și numai dacă*

$$a^{\frac{c}{d}} \equiv 1 \pmod{m}.$$

Demonstrație. Condiția $d \mid \operatorname{ind} a$ este echivalentă cu $\operatorname{ind} a \equiv 0 \pmod{d}$ și aceasta este echivalentă cu $\frac{c}{d} \operatorname{ind} a \equiv 0 \left(\operatorname{mod} \frac{c}{d} d\right)$, adică cu $\frac{c}{d} \operatorname{ind} a \equiv 0 \pmod{c}$, deoarece $\frac{c}{d} \neq 0$. Dar $\frac{c}{d} \operatorname{ind} a \equiv 0 \pmod{c}$ este echivalentă cu $g^{\frac{c}{d} \operatorname{ind} a} \equiv 1 \pmod{m}$, dacă g este baza în raport cu care se ia $\operatorname{ind} a$ modulo m, ținînd seama și de faptul că c este ordinul clasei de resturi modulo m, primă cu modulul reprezentată de g. Relația $g^{\frac{c}{d} \operatorname{ind} a} \equiv 1 \pmod{m}$ este însă același lucru cu relația $a^{\frac{c}{d}} \equiv 1 \pmod{m}$.

6.4. Indici modulo $\pm 2^\alpha$, α fiind un număr întreg nenegativ

Toate cele spuse mai sus rămîn valabile pentru $\pm 2^\alpha$ cu $\alpha = 0, 1, 2$, pentru că în aceste cazuri avem rădăcini primitive modulo $\pm 2^\alpha$. Rezultatele obținute în acest caz se înglobează însă în cazul general cînd α este număr întreg nenegativ, ceea ce rezultă din cele ce urmează.

În cazul cînd $\alpha \geqslant 3$ am arătat că orice număr întreg a prim cu 2, deci și cu $\pm 2^\alpha$ satisface congruența

$$a^{\frac{1}{2}\varphi(\pm 2^\alpha)} \equiv 1 \pmod{\pm 2^\alpha}.$$

Să arătăm că există un număr întreg a, prim cu $\pm 2^\alpha$, care reprezintă o clasă de resturi modulo $\pm 2^\alpha$, primă cu modulul, de ordin $\delta = \frac{1}{2}\varphi(\pm 2^\alpha)$ în cazul cînd $\alpha \geqslant 3$.

Teoremă. *Numărul 5 reprezintă o clasă de resturi modulo $\pm 2^\alpha$, primă cu modulul, de ordin $\frac{1}{2}\varphi(\pm 2^\alpha)$ dacă $\alpha \geqslant 3$.*

Demonstrație. Avem $5 = 1+4$, deci $5^2 = 1+8+16$. Aceste relații ne sugerează să demonstrăm prin inducție completă relația

$$5^{2^n} = 1 + 2^{n+2} + 2^{n+3} u_n,$$

unde n este un număr întreg nenegativ, iar u_n este un număr întreg. Relația scrisă este adevărată pentru $n=0$, deoarece ea se reduce la $5 = 1+4$ cu $u_0 = 0$. Să o presupunem adevărată pentru $n = i$. Avem deci $5^{2^i} = 1 + 2^{i+2} + 2^{i+3} u_i$. Atunci $(5^{2^i})^2 = (1 + 2^{i+2} + 2^{i+3} u_i)^2$, deci $5^{2^{i+1}} = 1 + 2 \cdot 2^{i+2} + 2 \cdot 2^{i+3} u_i + 2 \cdot 2^{i+2} \cdot 2^{i+3} u_i + 2^{2(i+2)} + (2^{i+3} u_i)^2 = 1 + 2^{i+3} + 2^{i+4}(u_i + 2^{i+2} u_i + 2^i + 2^{i+2} u_i^2) = 1 + 2^{i+3} + 2^{i+4} u_{i+1}$, unde am notat $u_{i+1} = u_i + 2^{i+2} u_i + 2^i + 2^{i+2} u_i^2$ care este un număr întreg. Proprietatea este deci adevărată și pentru $n = i+1$, deci este adevărată pentru orice n.

Fie δ ordinul clasei de resturi modulo $\pm 2^\alpha$, primă cu modulul reprezentată de 5. În cazul cînd $\alpha \geqslant 3$ avem $\delta \mid \frac{1}{2}\varphi(\pm 2^\alpha)$, deoarece în acest caz $5^{\frac{1}{2}\varphi(\pm 2^\alpha)} \equiv 1 \pmod{\pm 2^\alpha}$. Deci $\delta \mid 2^{\alpha-2}$, deoarece $\frac{1}{2}\varphi(\pm 2^\alpha) = \frac{1}{2} 2^{\alpha-1} = 2^{\alpha-2}$. Rezultă că $\delta = 2^r$, unde r este un număr întreg nenegativ astfel încît

$$r \leqslant \alpha - 2.$$

Dacă prin absurd $r < \alpha - 2$, atunci $r \leqslant \alpha - 3$ și deci $5^\delta \equiv 1 \pmod{\pm 2^\alpha}$ ne dă $5^{2^r} \equiv 1 \pmod{\pm 2^\alpha}$, de unde prin ridicări succesive la puterea a doua obținem

$$5^{2^{\alpha-3}} \equiv 1 \pmod{\pm 2^\alpha}.$$

Dar dacă în $5^{2^n} = 1 + 2^{n+2} + 2^{n+3} u_n$ luăm $n = \alpha - 3$ obținem $5^{2^{\alpha-3}} = 1 + 2^{\alpha-1} + 2^\alpha u_{\alpha-3}$, deci $5^{2^{\alpha-3}} \equiv 1 + 2^{\alpha-1} \pmod{\pm 2^\alpha}$, deci $1 + 2^{\alpha-1} \equiv 1 \pmod{\pm 2^\alpha}$ sau $2^{\alpha-1} \equiv 0 \pmod{\pm 2^\alpha}$, ceea ce este contradictoriu. Așadar $r = \alpha - 2$, deci $\delta = 2^{\alpha-2} = \frac{1}{2}\varphi(\pm 2^\alpha)$ și deci 5 reprezintă o clasă de resturi modulo $\pm 2^\alpha$, primă cu modulul, de ordin $\frac{1}{2}\varphi(\pm 2^\alpha)$ în cazul cînd $\alpha \geqslant 3$.

Teoremă. *Dacă* $\alpha \geqslant 2$, *atunci numerele*

$$5^0,\ 5^1,\ \ldots,\ 5^{2^{\alpha-2}-1}$$

$$-5^0,\ -5^1,\ \ldots,\ -5^{2^{\alpha-2}-1}$$

formează un sistem redus de resturi modulo $\pm 2^\alpha$.

Demonstrație. Într-adevăr, se constată că

(1) numărul numerelor de mai sus este egal cu $2 \cdot 2^{\alpha-2} = 2^{\alpha-1} = \varphi(\pm 2^\alpha)$;

(2) numerele de mai sus sînt necongruente două cîte două modulo $\pm 2^\alpha$. Într-adevăr, $5^i \not\equiv 5^j \pmod{\pm 2^\alpha}$, unde $0 \leqslant i \leqslant 2^{\alpha-2}-1$, $0 \leqslant j \leqslant 2^{\alpha-2}-1$, $i \neq j$, deoarece ordinul clasei de resturi modulo $\pm 2^\alpha$, primă cu modulul, reprezentată de 5 este $\frac{1}{2}\varphi(\pm 2^\alpha) = 2^{\alpha-2}$, dacă $\alpha \geqslant 3$, iar dacă $\alpha = 2$ avem numai 5^0 și deci nu există i și j cu $5^i \equiv 5^j \pmod{\pm 2^\alpha}$, $i \neq j$, $0 \leqslant i \leqslant 2^{\alpha-2}-1$, $0 \leqslant j \leqslant 2^{\alpha-2}-1$. Apoi $-5^i \not\equiv -5^j \pmod{\pm 2^\alpha}$, pentru același motiv, după ce suprimăm semnul minus. În fine $5^i \not\equiv -5^j \pmod{\pm 2^\alpha}$, deoarece din $5^i \equiv -5^j \pmod{\pm 2^\alpha}$ rezultă $5^i \equiv -5^j \pmod{2^2}$ cînd $\alpha \geqslant 2$ și deci $1 \equiv -1 \pmod 4$, deoarece $5^i \equiv 1 \pmod 4$, $-5^j \equiv -1 \pmod 4$, ceea ce nu se poate;

(3) numerele de mai sus sînt prime cu modulul $\pm 2^\alpha$.

Deci teorema este demonstrată.

Transcriind sub o altă formă această teoremă și înglobînd în ea și cazurile $\alpha = 0$, 1 obținem următoarea teoremă.

Teoremă. *Numerele* $(-1)^\gamma 5^{\gamma_0}$ *formează un sistem redus de resturi modulo* $\pm 2^\alpha$, α *fiind un număr întreg nenegativ, atunci cînd* γ *parcurge valorile* $0, 1, \ldots, c-1$, *iar* γ_0 *parcurge valorile* $0, 1, \ldots, c_0-1$, *unde* $c = 1$, $c_0 = 1$ *dacă* $\alpha = 0$ *sau* $\alpha = 1$ *și* $c = 2$, $c_0 = 2^{\alpha-2}$ *dacă* $\alpha \geqslant 2$.

Demonstrație. Pentru $\alpha \geqslant 2$, această teoremă este teorema precedentă. Pentru $\alpha = 0$ sau $\alpha = 1$ avem un singur număr de forma $(-1)^\gamma 5^{\gamma_0}$, anume: avem numărul $(-1)^0 5^0 = 1$ care constituie un sistem redus de resturi atît modulo $\pm 2^0$ cît și modulo $\pm 2^1$, deoarece $\varphi(\pm 2^0) = \varphi(\pm 2^1) = 1$, iar $(1, \pm 2^0) \cong 1$ și $(1, \pm 2^1) \cong 1$.

Se observă că $cc_0 = \varphi(\pm 2^\alpha)$ pentru orice α întreg nenegativ.

Teoremă. *Congruența*

$$(-1)^\gamma 5^{\gamma_0} \equiv (-1)^{\gamma'} 5^{\gamma_0} \pmod{\pm 2^\alpha}$$

este echivalentă cu sistemul de congruențe

$$\gamma \equiv \gamma' \pmod c,\quad \gamma_0 \equiv \gamma_0' \pmod{c_0}$$

unde γ, γ_0, γ', γ_0' *sînt numere întregi.*

Demonstrație. În cazul cînd $\alpha = 0$ sau $\alpha = 1$ avem $c = 1$, $c_0 = 1$, deci congruențele

$$\gamma \equiv \gamma' \pmod c,\quad \gamma_0 \equiv \gamma_0' \pmod{c_0}$$

sînt satisfăcute cu orice numere întregi γ, γ_0, γ' și γ_0'. Dacă $\alpha = 0$ sau $\alpha = 1$ avem

$$5 \equiv 1 \pmod{\pm 2^\alpha},$$

deci congruența $(-1)^\gamma 5^{\gamma_0} \equiv (-1)^{\gamma'} 5^{\gamma_0'} \pmod{\pm 2^\alpha}$ este echivalentă cu congruența $(-1)^\gamma \equiv (-1)^{\gamma'} \pmod{\pm 2^\alpha}$ care și ea este satisfăcută cu orice numere întregi γ, γ_0, γ' și γ_0', deoarece pentru $\alpha = 0$ avem $\pm 2^0 = \pm 1$ și deci $(-1)^\gamma$ este congruent cu $(-1)^{\gamma'}$ modulo ± 1, iar pentru $\alpha = 1$ avem $\pm 2^1 = \pm 2$, iar congruența $(-1)^\gamma \equiv (-1)^{\gamma'} \pmod{\pm 2^\alpha}$ devine una din congruențele $1 \equiv 1 \pmod{\pm 2}$, $-1 \equiv 1 \pmod{\pm 2}$, $1 \equiv -1 \pmod{\pm 2}$, $-1 \equiv -1 \pmod{\pm 2}$ care sînt adevărate.

Dacă $\alpha \geqslant 2$ scriem

$$\gamma = qc + r,\ 0 \leqslant r \leqslant c,\ \gamma_0 = q_0 c_0 + r_0,\ 0 \leqslant r_0 < c_0,$$

$$\gamma' = q'c + r',\ 0 \leqslant r' < c,\ \gamma_0' = q_0' c_0 + r_0',\ 0 \leqslant r_0' < c_0$$

și atunci obținem congruența

$$(-1)^r 5^{r_0} \equiv (-1)^{r'} 5^{r_0'} \pmod{\pm 2^\alpha}$$

care este echivalentă cu

$$(-1)^\gamma 5^{\gamma_0} \equiv (-1)^{\gamma} 5^{\gamma_0'} \pmod{\pm 2^\alpha},$$

deoarece $(-1)^\gamma 5^{\gamma_0} \equiv (-1)^{qc+r}\, 5^{q_0 c_0 + r_0} \equiv ((-1)^c)^q\ (-1)^r\, (5^{c_0})^{q_0} 5^{r_0} \equiv (-1)^r 5^{r_0} \pmod{\pm 2^\alpha}$ și $(-1)^{\gamma'} 5^{\gamma_0'} \equiv (-1)^{r'} 5^{r_0'} \pmod{\pm 2^\alpha}$, ceea ce se obține în mod analog, avînd în vedere că $c = 2$, deci $(-1)^c = 1$ și că $c_0 = 2^{\alpha-2}$ este ordinul clasei de resturi modulo $\pm 2^\alpha$, primă cu modulul, reprezentată de 5, în cazul cînd $\alpha \geqslant 3$, deci $5^{c_0} \equiv 1 \pmod{\pm 2^\alpha}$, ceea ce pentru $\alpha = 2$ se obține sub forma $5 \equiv 1 \pmod{\pm 2^2}$ avînd în vedere că pentru $\alpha = 2$ avem $c_0 = 1$.

Dar congruența

$$(-1)^r 5^{r_0} \equiv (-1)^{r'} 5^{r_0'} \pmod{\pm 2^\alpha}$$

este echivalentă cu $r=r'$, $r_0=r_0'$, conform teoremei precedente, ceea ce este echivalent cu

$$\gamma\equiv\gamma' \pmod{c},\ \gamma_0\equiv\gamma_0' \pmod{c_0}$$

conform celei de a doua definiții a relației de congruență.

Cele de mai sus ne inspiră următoarea definiție.

Definiție. *Dacă a este un număr întreg prim cu $\pm 2^\alpha$, atunci sistemul de numere întregi γ, γ_0 dat prin*

$$a\equiv(-1)^\gamma 5^{\gamma_0} \pmod{\pm 2^\alpha}$$

este sistem de indici ai numărului a modulo $\pm 2^\alpha$.

Observație. Există un sistem de indici modulo $\pm 2^\alpha$ pentru orice număr întreg prim cu $\pm 2^\alpha$, deoarece clasa de resturi modulo $\pm 2^\alpha$, primă cu modulul, reprezentată de a este reprezentată și de un număr întreg de forma $(-1)^\gamma 5^{\gamma_0}$, unde γ este un număr întreg din 0, 1, ..., $c-1$, iar γ_0 este un număr întreg din 0, 1, ..., c_0-1, conform teoremei anteprecedente.

Sistemul de indici al lui a modulo $\pm 2^\alpha$ este unic în sensul teoremei precedente, anume dacă γ, γ_0 și γ', γ_0' sînt sisteme de indici ai lui a modulo $\pm 2^\alpha$, atunci

$$\gamma\equiv\gamma' \pmod{c},\ \gamma_0\equiv\gamma_0' \pmod{c_0}.$$

Proprietăți ale sistemului de indici modulo $\pm 2^\alpha$.

(1) *Numerele întregi dintr-o clasă de resturi modulo $\pm 2^\alpha$, primă cu modulul, au un același sistem de indici modulo $\pm 2^\alpha$ și numai ele au un sistem de indici dat.*

Într-adevăr, dacă $a\equiv(-1)^\gamma 5^{\gamma_0} \pmod{\pm 2^\alpha}$, iar $b\equiv a \pmod{\pm 2^\alpha}$ atunci și $b\equiv(-1)^\gamma 5^{\gamma_0} \pmod{\pm 2^\alpha}$. Reciproc, dacă $a\equiv(-1)^\gamma 5^{\gamma_0} \pmod{\pm 2^\alpha}$ și $b\equiv(-1)^\gamma 5^{\gamma_0} \pmod{\pm 2^\alpha}$ atunci $a\equiv b \pmod{\pm 2^\alpha}$. Mai trebuie adăugat că fiind dat sistemul de numere întregi γ, γ_0 există un număr întreg prim cu $\pm 2^\alpha$ care să aibă pe γ, γ_0 ca sistem de indici modulo $\pm 2^\alpha$, deoarece un asemenea număr este $(-1)^\gamma 5^{\gamma_0}$.

(2) *Dacă $\gamma(a)$, $\gamma_0(a)$ este un sistem de indici modulo $\pm 2^\alpha$ ai numărului întreg a, iar $\gamma(b)$, $\gamma_0(b)$ este un sistem de indici modulo $\pm 2^\alpha$ ai numărului întreg b, atunci $\gamma(a)+\gamma(b)$, $\gamma_0(a)+\gamma_0(b)$ este un sistem de indici modulo $\pm 2^\alpha$ ai numărului întreg ab.*

Într-adevăr, dacă $a\equiv(-1)^{\gamma(a)} 5^{\gamma_0(a)} \pmod{\pm 2^\alpha}$, iar $b\equiv(-1)^{\gamma(b)} 5^{\gamma_0(b)} \pmod{\pm 2^\alpha}$, atunci $ab\equiv(-1)^{\gamma(a)+\gamma(b)} 5^{\gamma_0(a)+\gamma_0(b)} \pmod{\pm 2^\alpha}$.

În particular, *dacă γ, γ_0 este un sistem de indici modulo $\pm 2^\alpha$ ai numărului întreg a, atunci $n\gamma$, $n\gamma_0$ este un sistem de indici modulo $\pm 2^\alpha$ ai numărului întreg a^n.*

6.5. Indici în raport cu un modul diferit de zero

Fie $m\neq 0$. Putem scrie

$$m=\varepsilon 2^\alpha p_1^{\alpha_1}\dots p_r^{\alpha_r},$$

unde $\varepsilon=\pm 1$, 2, $p_1, \dots, p_r$ sînt numere prime pozitive diferite două cîte două, iar $\alpha_1, \dots, \alpha_r$ sînt numere naturale, α fiind număr întreg nenegativ. Vom pune $c=1$, $c_0=1$ dacă $\alpha=0$ sau $\alpha=1$ și $c=2$, $c_0=2^{\alpha-2}$ dacă $\alpha\geqslant 2$. Vom mai pune $c_i=\varphi(p_i^{\alpha_i})$ $(i=1,\dots,r)$, iar cu g_i vom nota o rădăcină primitivă modulo $p_i^{\alpha_i}$.

Definiție. *Dacă a este un număr întreg prim cu m atunci sistemul de numere întregi γ, γ_0, $\gamma_1, \dots, \gamma_r$* dat prin

$$a\equiv (-1)^\gamma 5^{\gamma_0} \pmod{2^\alpha},$$
$$a\equiv g_1^{\gamma_1} \pmod{p_1^{\alpha_1}},$$
$$\dots\dots\dots\dots\dots\dots\dots\dots$$
$$a\equiv g_r^{\gamma_r} \pmod{p_r^{\alpha_r}},$$

este sistem de indici ai numărului întreg a modulo m.

Observație. Există un sistem de indici modulo m pentru orice număr întreg a prim cu m, deoarece din faptul că $(a, m)\cong 1$ rezultă $(a, 2^\alpha)\cong 1$, $(a, p_i^{\alpha_i})\cong 1$ $(i=1,\dots, r)$, iar γ, γ_0 este sistem de indici ai lui a modulo 2^α, γ_i $(i=1,\dots, r)$ fiind indice al lui a modulo p_i $(i=1,\dots, r)$.

Sistemul de indici ai lui a modulo m este unic în sensul că dacă γ, γ_0, $\gamma_1, \dots, \gamma_r$ și γ', γ_0', $\gamma_1', \dots, \gamma_r'$ sînt sisteme de indici ai lui a modulo m, atunci

$$\gamma\equiv\gamma' \pmod{c},$$
$$\gamma_0\equiv\gamma_0' \pmod{(c_0)},$$
$$\gamma_i\equiv\gamma_i' \pmod{c_i}\ (i=1,\dots, r),$$

acest lucru rezultînd din faptul că γ, γ_0 și γ', γ_0' sînt sisteme de indici ai lui a modulo 2^α, iar γ_i, γ_i' $(i=1,\ldots,r)$ sînt indici ai lui a modulo $p_i^{\alpha_i}$ $(i=1,\ldots,r)$.

Proprietăți ale sistemului de indici modulo m.

(1) *Numerele întregi dintr-o clasă de resturi modulo* m, *primă cu modulul, au un același sistem de indici modulo* m *și numai ele au un sistem de indici dat.*

Într-adevăr, dacă

$$a\equiv(-1)^{\gamma}5^{\gamma_0} \pmod{2^\alpha},$$

$$a\equiv g_i^{\gamma_i} \pmod{p_i^{\alpha_i}} \quad (i=1,\ldots,r). \tag{I}$$

iar $b\equiv a \pmod m$, atunci $b\equiv a \pmod{2^\alpha}$, $b\equiv a \pmod{p_i^{\alpha_i}}$ $(i=1,\ldots,r)$ și deci

$$b\equiv(-1)^{\gamma}5^{\gamma_0} \pmod{2^\alpha},$$

$$b\equiv g_i^{\gamma_i} \pmod{p_i^{\alpha_i}} (i=1,\ldots,r). \tag{II}$$

Reciproc, dacă avem (I) și (II) obținem $a\equiv b \pmod{2^\alpha}$, $a\equiv b \pmod{p_i^{\alpha_i}}$ $(i=1,\ldots,r)$, deci $2^\alpha|a-b$, $p_i^{\alpha_i}|a-b$ $(i=1,\ldots,r)$, deci $m|a-b$, deoarece m este cel mai mic multiplu comun al numerelor întregi 2^α, $p_i^{\alpha_i}(i=1,\ldots,r)$. Deci $a\equiv b \pmod m$. Pentru ca demonstrația reciprocei să fie completă, mai trebuie dovedit că există cel puțin un număr întreg prim cu m pentru care sistemul de numere întregi γ, γ_0, $\gamma_1,\ldots,\gamma_r$ să constituie un sistem de indici modulo m. Cu alte cuvinte, trebuie arătat că sistemul de congruențe

$$x\equiv(-1)^{\gamma}5^{\gamma_0} \pmod{2^\alpha},$$

$$x\equiv g_i^{\gamma_i} \pmod{p_i^{\alpha_i}} \quad (i=1,\ldots,r)$$

admite ca soluție un număr întreg prim cu m. Acest sistem de congruențe admite un număr întreg ca soluție, deoarece modulii 2^α, $p_i^{\alpha_i}(i=1,\ldots,r)$ sînt primi doi cîte doi. Această soluție este primă cu m, deoarece este primă cu 2^α, $p_i^{\alpha_i}$ $(i=1,\ldots,r)$, numerele $(-1)^{\gamma}5^{\gamma_0}$, $g_i^{\gamma_i}(i=1,\ldots,r)$ fiind prime respectiv cu 2^α, $p_i^{\alpha_i}$ $(i=1,\ldots,r)$.

(2) *Dacă* $\gamma(a)$, $\gamma_0(a)$, $\gamma_1(a),\ldots,\gamma_r(a)$ *este un sistem de indici modulo* m *ai numărului întreg* a, *iar* $\gamma(b)$, $\gamma_0(b)$, $\gamma_1(b),\ldots,\gamma_r(b)$ *este un sistem de indici modulo* m *ai numărului întreg* b, *atunci* $\gamma(a)+\gamma(b)$, $\gamma_0(a)+\gamma_0(b)$, $\gamma_1(a)+\gamma_1(b),\ldots,\gamma_r(a)+\gamma_r(b)$ *este un sistem de indici modulo* m *ai numărului întreg* ab.

Într-adevăr, dacă $a\equiv(-1)^{\gamma(a)}5^{\gamma_0(a)} \pmod{2^\alpha}$, $a\equiv g_i^{\gamma_i(a)} \pmod{p_i^{\alpha_i}}$ $(i=1,\ldots,r)$, iar $b\equiv(-1)^{\gamma(b)}5^{\gamma_0(b)} \pmod{2^\alpha}$, $b\equiv g_i^{\gamma_i(b)} \pmod{p_i^{\alpha_i}}$ $(i=1,\ldots,r)$, atunci $ab\equiv(-1)^{\gamma(a)+\gamma(b)}5^{\gamma_0(a)+\gamma_0(b)} \pmod{2^\alpha}$, $ab\equiv g_i^{\gamma_i(a)+\gamma_i(b)} \pmod{p_i^{\alpha_i}}$ $i=1,\ldots,r)$.

În particular, *dacă* γ, γ_0, $\gamma_1,\ldots,\gamma_r$ *este un sistem de indici modulo* m *ai numărului întreg* a *atunci* $n\gamma$, $n\gamma_0$, $n\gamma_1,\ldots,n\gamma_r$ *este un sistem de indici modulo* m *ai numărului întreg* a^n.

Capitolul 7

FUNCȚII NUMERICE

7.1. Definiția funcțiilor numerice

O funcție numerică este o funcție care are ca domeniu mulțimea numerelor întregi sau reale, iar drept codomeniu mulțimea numerelor complexe. În unele cazuri, valorile unei astfel de funcții sînt numere reale sau numere întregi sau chiar numere naturale.

Exemple. Funcția *signum* definită în felul următor:

$$\operatorname{sign} a = \begin{cases} 1 \text{ dacă } a>0, \\ 0 \text{ dacă } a=0, \\ -1 \text{ dacă } a<0, \end{cases}$$

unde a este un număr întreg, este o funcție numerică. Valorile acestei funcții sînt numerele întregi -1, 0, 1.

Funcția *valoare absolută* definită în felul următor

$$|a| = \begin{cases} a \text{ dacă } a>0, \\ 0 \text{ dacă } a=0, \\ -a \text{ dacă } a<0, \end{cases}$$

unde a este un număr întreg, este o funcție numerică. Valorile acestei funcții sînt numere naturale și numărul 0.

Funcția lui Euler, adică indicatorul lui Euler al unui număr întreg, este o funcție numerică. Valorile acestei funcții sînt numere naturale.

Funcții numerice multiplicative și total-multiplicative.

Definiție. *O funcție numerică $f(a)$ este total-multiplicativă dacă*

$$f(mn)=f(m)\ f(n),$$

oricare ar fi perechea m, n de numere întregi.

Definiție. *O funcție numerică $f(a)$ este multiplicativă dacă*

$$f(mn)=f(m)\,f(n),$$

oricare ar fi perechea m, n de numere întregi pentru care

$$(m,\ n)\cong 1.$$

Observație. Orice funcție numerică total-multiplicativă este și multiplicativă, deoarece relația $f(mn)=f(m)\,f(n)$ verificîndu-se pentru toate perechile m, n de numere întregi, se verifică și pentru toate perechile m, n de numere întregi pentru care $(m, n)\cong 1$. Reciproca nu este adevărată, deoarece perechile m, n de numere întregi pentru care $(m, n)\cong 1$ formează o submulțime proprie a mulțimii perechilor m, n de numere întregi.

Exemple. Funcția signum este total-multiplicativă din cauza regulii semnelor

$$\operatorname{sign}(mn)=\operatorname{sign} m\ \operatorname{sign} n.$$

Funcția valoare absolută este, de asemenea, total-multiplicativă din cauză că

$$|mn|=|m|\ |n|.$$

În schimb, funcția lui Euler este numai multiplicativă, deoarece

$$\varphi(mn)=\varphi(m)\ \varphi(n)$$

dacă $(m, n)\cong 1$. Există cazuri cînd $(m, n)\ncong 1$, iar $\varphi(mn)\neq\varphi(m)\ \varphi(n)$. Un astfel de caz este pentru $m=0$, $n=0$, deoarece $(0, 0)\ncong 1$, iar $\varphi(0\cdot 0)\neq\varphi(0)\ \varphi(0)$ avînd $2\neq 2\cdot 2$.

Funcția de sumare a unei funcții numerice.

Definiție. *Funcția de sumare a unei funcții numerice f este o funcție F definită prin*

$$F(n)=\sum_{d|n} f(d)$$

pentru orice număr întreg $n\neq 0$, suma fiind extinsă la mulțimea divizorilor pozitivi ai lui n, fiecare divizor pozitiv fiind luat o singură dată. Dacă $n=0$, considerăm că $F(0)=0$ sau $F(0)=1$ dacă și $F(\pm)=1$.

Teoremă. *Avem*

$$\sum_{d|a} f(d)=\sum_{d_1|m}\Big(\sum_{d_2|n} f(d_1d_2)\Big),$$

dacă $a\neq 0$, $a=mn$, iar $(m, n)\cong 1$.

Demonstrație. În cazul $a\neq 0$, $a=mn$ și $(m, n)\cong 1$, notăm cu M mulțimea tuturor divizorilor pozitivi ai lui a, $M=\{d|d>0 \,\&\, d|a\}$, iar cu N mulțimea tuturor produselor d_1d_2, unde $d_1>0$, $d_2>0$, $d_1|m$, $d_2|n$, $N=\{d_1d_2|d_1>0\,\&\,d_2>0\,\&\,d_1|m\,\&\,d_2|n\}$. Vom arăta că $M=N$. Într-adevăr, fie $d\in M$. Deci $d>0$ și $d|a$. Cum $a=mn$ rezultă că $d|mn$. Luăm $d_1\cong(d, m)$, $d_1>0$. Putem lua $d_1>0$, deoarece $m\neq 0$ ca urmare a faptului că $a\neq 0$. Deci $d=d_1d_2$ și $m=d_1e$, unde $(d_2, e)\cong 1$, deoarece $m\neq 0$. Din $d|mn$ deducem acum că $d_1d_2|d_1en$, deci $d_2|en$, deoarece $d_1\neq 0$, deci $d_2|n$, deoarece $(d_2, e)\cong 1$. Avem și $d_2>0$, deoarece $d=d_1d_2$ și $d>0$, $d_1>0$. Am dovedit deci că dacă $d\in M$, atunci $d=d_1d_2$, unde $d_1>0$, $d_2>0$, $d_1|m$, $d_2|n$, deci $d\in N$, așa că $M\subseteq N$.

Fie acum $d_1d_2\in N$. Asta înseamnă că $d_1>0$, $d_2>0$, $d_1|m$, $d_2|n$. Dar atunci $d_1d_2|mn$ și $d_1d_2>0$ deci $d_1d_2\in M$, deci $N\subseteq M$ și am dovedit că $M=N$.

Numerele d după care se face suma $\sum_{d|a} f(d)$ formează mulțimea M și fiecare din ele apare o singură dată în suma considerată, conform definiției sumei $\sum_{d|a} f(d)$. Numerele d_1d_2 după care se face suma $\sum_{d_1|m}\big(\sum_{d_2|n} f(d_1d_2)\big)$ formează mulțimea N. Dacă arătăm că fiecare din numerele d_1d_2 apare o singură dată în suma considerată, atunci din faptul că $M=N$ rezultă că cele două sume sînt identice. Însă din $d_1d_2\in N$ și $d_1'd_2'\in N$ cu $d_1d_2=d_1'd_2'$ deducem $d_1=d_1'$, $d_2=d_2'$. Într-adevăr, dacă $d_1d_2=d_1'd_2'$ avem $d_1|d_1'd_2'$. Din cauză că $d_1|m$ deducem $m=d_1m_1$ și din cauză că $d_2'|n$ deducem $n=d_2'n_2'$. Apoi,

ținînd seama de $(m, n)\cong 1$, deducem $(d_1m_1, d_2'n_2')\cong 1$, deci $(d_1m_1, d_2')\cong 1$, deci $(d_1, d_2')\cong 1$. Așadar, din $d_1|d_1'd_2'$ deducem $d_1|d_1'$. În mod analog, stabilim că $d_1'|d_1$ și cum $d_1>0$, $d_1'>0$ rezultă că $d_1=d_1'$ deci și $d_2=d_2'$. Cu aceasta teorema este demonstrată.

Teoremă. *Dacă funcția f este total-multiplicativă sau este numai multiplicativă, atunci funcția sa de sumare este multiplicativă.*

Demonstrație. Fie

$$F(a)=\sum_{d|a} f(d).$$

În cazul cînd $a\neq 0$, $a=mn$, $(m, n)\cong 1$ avem

$$F(mn)=\sum_{d|a} f(d)=\sum_{d_1|m}\Big(\sum_{d_2|n} f\ (d_1d_2)\Big).$$

Putem scrie $f(d_1d_2)=f(d_1)\,f(d_2)$ în cazul cînd funcția f este total-multiplicativă, dar putem scrie și $f(d_1d_2)=f(d_1)\,f(d_2)$ în cazul cînd funcția este numai multiplicativă, ca urmare a faptului că din $d_1|m$, $d_2|n$ și $(m, n)\cong 1$ rezultă $(d_1, d_2)\cong 1$ scriind $m=d_1m_1$, $n=d_2n_2$, deci $(d_1m_1, d_2n_2)\cong 1$, deci $(d_1, d_2n_2)\cong 1$, deci $(d_1, d_2)\cong 1$. Așadar

$$F(mn)=\sum_{d_1|m}\Big[\sum_{d_2|n} f(d_1d_2)\Big]=\sum_{d_1|m}\Big(\sum_{d_2|n} f(d_1)\,f(d_2)\Big)=$$

$$=\sum_{d_1|m} f(d_1)\Big(\sum_{d_2|n} f(d_2)\Big)=\Big(\sum_{d_1|m} f(d_1)\Big)\Big(\sum_{d_2|n} f(d_2)\Big)=F(m)\,F(n).$$

Dacă $mn=0$, atunci $m=0$ sau $n=0$. Dacă $m=0$ avem $n=\pm 1$, deoarece $(m, n)\cong 1$, iar dacă $n=0$ avem $m=\pm 1$ pentru același motiv, deci

$$0=F(0)=F(0)\,F(\pm 1)=0\cdot F(\pm 1),$$

$$0=F(0)=F(\pm 1)\,F(0)=F(\pm 1)\cdot 0,$$

sau

$$1=F(0)=F(0)\,F(\pm 1)=1\cdot 1,$$

$$1=F(0)=F(\pm 1)\,F(0)=1\cdot 1.$$

În cele ce urmează, atît în acest capitol, cît și în cîteva din capitolele următoare vom da cîteva din funcțiile numerice utilizate în teoria numerelor.

7.2. Partea întreagă și partea fracționară ale unui număr real

Prima definiție a părții întregi și părții fracționare ale unui număr real. Dacă α este un număr real, partea întreagă a lui α este un număr întreg notat cu $[\alpha]$, iar partea fracționară a lui α este un număr real notat cu $\{\alpha\}$ astfel încît să fie satisfăcute relațiile

$$\alpha=[\alpha]+\{\alpha\},\quad 0\leqslant\{\alpha\}<1.$$

Teoremă. *Partea întreagă și partea fracționară ale unui număr real α sînt unic determinate.*

Demonstrație. Fie $\alpha=a+b$ și $\alpha=c+d$, unde a și c sînt numere întregi, iar b și d două numere reale astfel încît $0\leqslant b<1$ și $0\leqslant d<1$. Vom demonstra că $a=c$ și $b=d$.

Într-adevăr, avem $a+b=c+d$, deci $a-c=d-b$, deci $|a-c|=|d-b|$. Dar $|a-c|$ este un număr întreg. Apoi din $0\leqslant b<1$ și $0\leqslant d<1$ rezultă că $-1<-b\leqslant 0$ deci $-1<d-b<1$ sau $|d-b|<1$, deci singurul număr întreg nenegativ mai mic ca 1 fiind 0 avem $|a-c|=0$ deci $a-c=0$, deci $a=c$ și $d=b$.

A doua definiție a părții întregi și a părții fracționare ale unui număr real. Dacă α este un număr real, partea întreagă a lui α este un număr întreg notat cu $[\alpha]$, iar partea fracționară a lui α este un număr real notat cu $\{\alpha\}$ astfel încît să fie satisfăcute relațiile

$$[\alpha]\leqslant\alpha<[\alpha]+1,\quad \{\alpha\}=\alpha-[\alpha].$$

Teoremă. *Cele două definiții sînt echivalente.*

Demonstrație. Din prima definiție rezultă că $\alpha=[\alpha]+\{\alpha\}\geqslant[\alpha]$, deoarece $0\leqslant\{\alpha\}$ și $\alpha=[\alpha]+\{\alpha\}<[\alpha]+1$, deoarece $\{\alpha\}<1$, deci rezultă

$$[\alpha]\leqslant\alpha<[\alpha]+1,\quad \{\alpha\}=\alpha-[\alpha],$$

$[\alpha]$ fiind un număr întreg, ceea ce constituie a doua definiție.

Din a doua definiție rezultă $0\leqslant\alpha-[\alpha]<1$. Notînd $\alpha-[\alpha]=\{\alpha\}$ obținem

$$\alpha=[\alpha]+\{\alpha\},\quad 0\leqslant\{\alpha\}<1,$$

$[\alpha]$ fiind un număr întreg, ceea ce constituie prima definiție.

Vom stabili următoarele proprietăți:

Teoremă. *Pentru orice număr real α avem*

$$[\alpha]-2\left[\frac{\alpha}{2}\right]\geqslant 0.$$

Demonstrație. Avem $\frac{\alpha}{2}=\left[\frac{\alpha}{2}\right]+\left\{\frac{\alpha}{2}\right\}$ cu $0\leqslant\left\{\frac{\alpha}{2}\right\}<1$, deci $\alpha=2\left[\frac{\alpha}{2}\right]+2\left\{\frac{\alpha}{2}\right\}$. Dacă $0\leqslant\left\{\frac{\alpha}{2}\right\}<\frac{1}{2}$, atunci $0\leqslant 2\left\{\frac{\alpha}{2}\right\}<1$, deci $[\alpha]=2\left[\frac{\alpha}{2}\right]$, datorită unicității părții întregi, deci $[\alpha]-2\left[\frac{\alpha}{2}\right]\geqslant 0$. Dacă $\frac{1}{2}\leqslant\left\{\frac{\alpha}{2}\right\}<1$, atunci $1\leqslant 2\left\{\frac{\alpha}{2}\right\}<2$, deci $0\leqslant 2\left\{\frac{\alpha}{2}\right\}-1<1$. Atunci scriind $\alpha=2\left[\frac{\alpha}{2}\right]+1+\left(2\left\{\frac{\alpha}{2}\right\}-1\right)$ constatăm, datorită unicității părții întregi, că $[\alpha]=2\left[\frac{\alpha}{2}\right]+1$, deci $[\alpha]-2\left[\frac{\alpha}{2}\right]=1$ deci $[\alpha]-2\left[\frac{\alpha}{2}\right]\geqslant 0$.

Teoremă. *Pentru orice număr real α și orice număr natural n avem*

$$\left[\frac{\alpha}{n}\right]=\left[\frac{[\alpha]}{n}\right].$$

Demonstrație. $\alpha=[\alpha]+\{\alpha\}$ cu $0\leqslant\{\alpha\}<1$, deci $\frac{\alpha}{n}=\frac{[\alpha]}{n}+\frac{\{\alpha\}}{n}$. Însă $\frac{[\alpha]}{n}=\left[\frac{[\alpha]}{n}\right]+\left\{\frac{[\alpha]}{n}\right\}$ cu $0\leqslant\left\{\frac{[\alpha]}{n}\right\}<1$, deci $\frac{\alpha}{n}=\left[\frac{[\alpha]}{n}\right]+\left(\left\{\frac{[\alpha]}{n}\right\}+\frac{\{\alpha\}}{n}\right)$. Să arătăm că $0\leqslant\left\{\frac{[\alpha]}{n}\right\}+\frac{\{\alpha\}}{n}<1$. Aplicînd teorema împărțirii întregi lui $[\alpha]$ și n obținem $[\alpha]=nq+r$, $0\leqslant r<n$, deci $\frac{[\alpha]}{n}=q+\frac{r}{n}$, deci $\frac{r}{n}=\left\{\frac{[\alpha]}{n}\right\}$, avînd $0\leqslant\frac{r}{n}<1$, q fiind număr întreg. Avem $r\leqslant n-1$, deci $\frac{r}{n}\leqslant\frac{n-1}{n}=1-\frac{1}{n}$. Deci $0\leqslant\left\{\frac{[\alpha]}{n}\right\}+\frac{\{\alpha\}}{n}\leqslant 1-\frac{1}{n}+\frac{\{\alpha\}}{n}=1-\frac{1-\{\alpha\}}{n}<1$, deoarece $1-\{\alpha\}>0$. Din cauza uni-

citații părții întregi, din $\frac{\alpha}{n}=\left[\frac{[\alpha]}{n}\right]+\left(\left\{\frac{[\alpha]}{n}\right\}+\frac{\{\alpha\}}{n}\right)$ și $0\leqslant\left\{\frac{[\alpha]}{n}\right\}+\frac{\{\alpha\}}{n}<1$, rezultă

$$\left[\frac{\alpha}{n}\right]=\left[\frac{[\alpha]}{n}\right].$$

Teoremă. *În descompunerea în factori primi a lui n!, anume în*

$$n!=\prod_p p^{e_p},$$

avem $e_p=\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\ldots$

Demonstrație. Să dăm, mai întîi, cîteva explicații în legătură cu formularea teoremei. Prin scrierea $n!=\prod_p p^{e_p}$ înțelegem următoarea scriere $n!=2^{e_2}3^{e_3}5^{e_5}7^{e_7}\ldots$, adică toți factorii primi pozitivi sînt scriși în ordine crescătoare cu exponenți egali cu exponenții numerelor prime, cu care sînt asociați, din descompunerea în factori primi a lui $n!$. Acei factori primi pozitivi p care nu figurează în descompunerea în factori primi a lui $n!$, figurează în $n!=\prod_p p^{e_p}$ cu exponentul egal cu zero.

Suma $e_p=\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\ldots$, o concepem ca o serie, adică e_p este limita șirului de sume parțiale $\left[\frac{n}{p}\right]$, $\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]$, $\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\left[\frac{n}{p^3}\right],\ldots$ Sumele e_p sînt însă sume finite, deoarece pentru orice număr prim p pozitiv putem lua

$$s=\left[\frac{\log n}{\log p}\right],$$

deci $s\leqslant\frac{\log n}{\log p}<s+1$, deci $s\log p\leqslant\log n<(s+1)\log p$, deoarece $\log p>0$. Așadar $\log p^s\leqslant\log n<\log p^{s+1}$, deci $p^s\leqslant n<p^{s+1}$. Pentru orice număr întreg r, $r>s$, avem $r\geqslant s+1$, deci $p^r\geqslant p^{s+1}$ deoarece $p>1$. Deci pentru orice număr întreg r, $r>s$, avem

$$p^r>n.$$

Atunci $0<\frac{n}{p^r}<1$, deci $\left[\frac{n}{p^r}\right]=0$, deci

$$e_p=\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\ldots+\left[\frac{n}{p^s}\right]$$

este o sumă finită.

Să trecem, acum, la demonstrația teoremei. Fie p un număr prim pozitiv. Exponentul e_p cu care p intră în descompunerea în factori primi a lui $n!$ este

$$e_p=1\cdot k_1+2\cdot k_2\ldots,$$

unde k_1 este numărul numerelor luate dintre $1,\ldots,n$ care se divid cu p la puterea 1 și nu se divid cu p la puterea 2, unde k_2 este numărul numerelor luate dintre $1,\ldots,n$ care se divid cu p la puterea 2 și nu se divid cu p la puterea 3 etc. Într-adevăr, exponenții 1 trebuie adunați de k_1 ori, exponenții 2 trebuie adunați de k_2 ori etc.

Să calculăm pe k_i. Numerele care se divid cu p^i și sînt luate din $1,\ldots,n$ sînt

$$1\cdot p^i,\ 2\cdot p^i,\ \ldots,\ t_ip^i,$$

cu $t_ip^i\leqslant n<(t_i+1)p^i$, deoarece dacă j este luat din $1,\ldots,n$ și $p^i|j$ avem $j=tp^i$, t fiind un număr întreg, și cum $1\leqslant j\leqslant n$ avem $1\leqslant tp^i\leqslant n$. Dar

$$t_i\leqslant\frac{n}{p^i}<t_i+1,$$

deci $t_i=\left[\frac{n}{p^i}\right]$. Numerele luate din $1,\ldots,n$ care se divid cu p^{i+1} se află toate printre numerele luate din $1,\ldots,n$ care se divid cu p^i. Dacă din numerele luate din $1,\ldots,n$ care se divid cu p^i, care sînt în număr de t_i, extragem toate numerele luate din $1,\ldots,n$ care se divid cu p^{i+1}, care sînt în număr de $t_{i+1}=\left[\frac{n}{p^{i+1}}\right]$, obținem numai numerele luate din $1,\ldots,n$ care se divid cu p^i, dar nu se divid cu o putere mai mare a lui p, deoarece nu se divid cu p^{i+1}. Conform celor spuse mai sus, numărul acestor numere este egal cu $k_i=t_i-t_{i+1}$. Avem deci

$$e_p=1\cdot(t_1-t_2)+2\cdot(t_2-t_3)+\ldots=$$

$$=t_1+t_2+t_3+\ldots=\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\left[\frac{n}{p^3}\right]+\ldots$$

Exemplu. $6!=2^4 3^2 5$, deoarece

$$\left[\frac{6}{2}\right]=[3]=3,\left[\frac{6}{2^2}\right]=\left[\frac{6}{4}\right]=1,\left[\frac{6}{2^3}\right]=\left[\frac{6}{8}\right]=0;\left[\frac{6}{3}\right]=[2]=2,$$

$$\left[\frac{6}{3^2}\right]=\left[\frac{6}{9}\right]=0;\left[\frac{6}{5}\right]=1,\left[\frac{6}{5^2}\right]=0;\left[\frac{6}{7}\right]=0.$$

$$e_2=3+1=4,\ e_3=2,\ e_5=1.$$

Observație. Dacă $p>n$, atunci $e_p=0$. Acest lucru rezultă direct din teorema unicității descompunerii în factori primi. Într-adevăr, dacă $p>n$ atunci $p\nmid n!$, deoarece în caz contrar, din $p|n!$ rezultă $p|j$ cu $1\leqslant j\leqslant n$, deci $p\leqslant j\leqslant n$ sau $p\leqslant n$ în contrazicere cu $p>n$. Dar $e_p=0$ rezultă și din formula $e_p=\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\ldots$ deoarece avînd $p>n$, avem $p^m\geqslant p>n$ pentru orice m, $m\geqslant 1$, deci $\left[\frac{n}{p^m}\right]=0$, deoarece $0\leqslant\frac{n}{p^m}<1$, deci $e_p=0$.

7.3. Numărul divizorilor pozitivi

Numărul divizorilor pozitivi ai unui număr întreg, pe care îi putem numi și nenegativi dacă ne gîndim la divizorii nenegativi ai lui 0, ni-l dă o funcție numerică care se notează cu τ. Această funcție se definește în felul următor:

$$\tau(n)=\begin{cases}1 & \text{dacă } n=0,\\ (\alpha_1+1)\ldots(\alpha_r+1) & \text{dacă } n\neq 0 \text{ și } n=\pm p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_r^{\alpha_r},\end{cases}$$

numerele prime pozitive $p_1, p_2, \ldots, p_r$ fiind diferite două cîte două, $\alpha_1, \alpha_2, \ldots, \alpha_r$ fiind numere întregi nenegative.

Teoremă. *$\tau(n)$ reprezintă numărul divizorilor nenegativi ai numărului întreg n, cel mult egali cu n.*

Demonstrație. Dacă $n=0$, singurul divizor al lui 0, care este nenegativ și cel mult egal cu 0, este 0.

Dacă $n\neq 0$, numărul întreg n nu are pe 0 ca divizor, iar orice divizor pozitiv d al lui n se scrie sub forma $d=p_1^{\beta_1}p_2^{\beta_2}\ldots p_r^{\beta_r}$,

unde $\beta_1, \beta_2, \ldots, \beta_r$ sînt numere întregi nenegative, aceasta în cazul cînd $n=\pm p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_r^{\alpha_r}$ numerele întregi $\beta_1, \beta_2, \ldots, \beta_r$ satisfăcînd inegalitățile

$$0\leqslant\beta_1\leqslant\alpha_1,\ 0\leqslant\beta_2\leqslant\alpha_2,\ \ldots,\ 0\leqslant\beta_r\leqslant\alpha_r.$$

Acest lucru rezultă din aceea că dacă $d|n$, atunci $n=dc$. Deci factorii primi care figurează în d trebuie să figureze și în n altfel nu este satisfăcută unicitatea descompunerii în factori primi. Apoi factorii primi care figurează în d și n trebuie să figureze în d la o putere cel mult egală cu puterea factorului prim corespunzător din n, deoarece în caz contrar din nou nu este satisfăcută unicitatea descompunerii în factori primi. Pe de altă parte, dacă condițiile de mai sus sînt satisfăcute avem $d|n$, deoarece luînd $c=\pm p_1^{\alpha_1-\beta_1}p_2^{\alpha_2-\beta_2}\ldots p_r^{\alpha_r-\beta_r}$ obținem $n=dc$.

Deci β_1 poate lua α_1+1 valori, egale cu 0, 1, ..., α_1 ș.a.m.d., β_r poate lua α_r+1 valori, egale cu 0, 1, ..., α_r, deci numărul sistemelor de valori $\beta_1, \ldots, \beta_r$ este egal cu produsul $(\alpha_1+1)\ldots(\alpha_r+1)$. Deci numărul divizorilor pozitivi ai unui număr întreg $n\neq 0$ este egal cu numărul sistemelor de valori $\beta_1, \ldots, \beta_r$, deoarece la valori diferite ale sistemului $\beta_1, \ldots, \beta_r$ corespund numere naturale diferite din cauza unicității descompunerii în factori primi a numerelor întregi. Cu aceasta teorema este demonstrată.

Teoremă. *Funcția τ este multiplicativă.*

Demonstrație. Dacă $(m, n)\cong 1$ și $m\neq 0$, $n\neq 0$, atunci $m=\varepsilon_m p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_r^{\alpha_r}$, $n=\varepsilon_n p_{r+1}^{\alpha_{r+1}}p_{r+2}^{\alpha_{r+2}}\ldots p_s^{\alpha_s}$, unde $\varepsilon_m=\pm 1$, $\varepsilon_n=\pm 1$, $\alpha_1, \alpha_2, \ldots, \alpha_r, \alpha_{r+1}, \alpha_{r+2}, \ldots, \alpha_s$ sînt numere întregi nenegative, iar $p_1, p_2, \ldots, p_r, p_{r+1}, p_{r+2}, \ldots, p_s$ sînt numere prime pozitive, diferite două cîte două, deoarece $p_1, p_2, \ldots, p_r$ sînt diferite două cîte două, $p_{r+1}, p_{r+2}, \ldots, p_s$ sînt diferite două cîte două și oricare dintre $p_1, p_2, \ldots, p_r$ este diferit de oricare dintre $p_{r+1}, p_{r+2}, \ldots, p_s$, fiindcă dacă unul dintre $p_1, p_2, \ldots, p_r$ ar fi identic cu unul dintre $p_{r+1}, p_{r+2}, \ldots, p_s$, atunci valoarea p a unuia dintre ele ar divide și pe m și pe n și deci pe 1, pentru că $(m, n)\cong 1$, deci $p|1$, ceea ce este absurd, p fiind prim. Dar atunci

$$mn=\varepsilon_m\varepsilon_n p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_r^{\alpha_r}p_{r+1}^{\alpha_{r+1}}p_{r+2}^{\alpha_{r+2}}\ldots p_s^{\alpha_s},$$

deci

$$\tau(mn)=(\alpha_1+1)(\alpha_2+1)\ldots(\alpha_r+1)(\alpha_{r+1}+1)(\alpha_{r+2}+1)\ldots(\alpha_s+1)=\tau(m)\tau(n).$$

Dacă $m=0$, atunci $n=\pm 1$, iar dacă $n=0$, atunci $m=\pm 1$, deoarece $(m, n)\cong 1$, deci

$$1=\tau(0)=\tau(0)\ \tau(\pm 1)=1\cdot 1.$$

$$1=\tau(0)=\tau(\pm 1)\ \tau(0)=1\cdot 1.$$

7.4. Suma divizorilor pozitivi

Suma divizorilor pozitivi ai unui număr întreg, pe care îi putem numi și divizori nenegativi dacă ne referim la divizorii nenegativi ai lui 0, ne-o dă o funcție numerică care se notează cu σ. Această funcție se definește în felul următor:

$$\sigma(n)=\begin{cases} 0 \text{ dacă } n=0, \\ \sum\limits_{d|n} d \text{ dacă } n\neq 0. \end{cases}$$

Teoremă. *$\sigma(n)$ reprezintă suma divizorilor nenegativi ai numărului întreg n, cel mult egali cu n.*

Demonstrație. Dacă $n=0$, singurul divizor al lui 0, care este nenegativ și cel mult egal cu 0, este 0. Dacă $n\neq 0$, egalitatea $\sigma(n)=\sum\limits_{d|n} d$ demonstrează teorema.

Teoremă. *Funcția σ este multiplicativă.*

Demonstrație. Funcția σ este funcția de sumare a funcției $f(n)=n$ și avem $\sigma(0)=0$. Deoarece funcția $f(n)=n$ este total-multiplicativă, înseamnă că σ este multiplicativă.

Numere perfecte.

Definiție. *Un număr natural n este perfect dacă $\sigma(n)=2n$.*

Teoremă. *Condiția necesară și suficientă ca un număr natural par n să fie perfect este ca*

$$n=2^{\nu}(2^{\nu+1}-1),$$

ν fiind număr natural, iar $2^{\nu+1}-1$ număr prim.

Demonstrație. Condiția este necesară. Numărul natural n fiind par putem scrie pe n sub forma

$$n=2^{\nu}u,$$

unde ν este un număr natural, iar u este un număr impar, deoarece în descompunerea în factori primi a lui n putem separa factorul care este format dintr-o putere a lui 2. Avem $(2^{\nu}, u)\cong 1$, deoarece u este impar. Funcția σ fiind multiplicativă, avem $\sigma(2^{\nu}u)=\sigma(2^{\nu})\sigma(u)$. Însă

$$\sigma(2^{\nu})=\sum_{\delta=0}^{\nu} 2^{\delta}=\frac{2^{\nu+1}-1}{2-1}=2^{\nu+1}-1.$$

Deci $\sigma(n)=(2^{\nu+1}-1)\sigma(u)$. Numărul natural n fiind perfect, avem $\sigma(2^{\nu}u)=2(2^{\nu}u)=2^{\nu+1}u$. Deci $2^{\nu+1}u=(2^{\nu+1}-1)\sigma(u)$. Deci $2^{\nu+1}\mid(2^{\nu+1}-1)\sigma(u)$. Dar $(2^{\nu+1}, 2^{\nu+1}-1)\cong 1$, numărul $2^{\nu+1}-1$ fiind impar. Deci $2^{\nu+1}\mid\sigma(u)$, deci există un număr natural t astfel încît $\sigma(u)=2^{\nu+1}t$. Din $2^{\nu+1}u=(2^{\nu+1}-1)\sigma(u)$ deducem $u=(2^{\nu+1}-1)t$. Avem deci $\sigma(u)=\sum\limits_{d|u} d\geqslant(2^{\nu+1}-1)t+t+1>2^{\nu+1}t$ în cazul cînd $t>1$, deoarece atunci 1, t și $(2^{\nu+1}-1)t$ sînt divizori distincți ai lui $u=(2^{\nu+1}-1)t$ avînd $1\neq t$ pentru motivul că $t>1$, $1\neq(2^{\nu+1}-1)t$ pentru același motiv la care se adaugă și $2^{\nu+1}-1\geqslant 1$, $t\neq(2^{\nu+1}-1)t$ pentru motivul că $t<(2^{\nu+1}-1)t$ din cauză că $2^{\nu+1}-1>1$, ceea ce rezultă din $\nu\geqslant 1$. Dar $\sigma(u)>2^{\nu+1}t$ se contrazice cu $\sigma(u)=2^{\nu+1}t$, deci $t=1$. Deci $u=2^{\nu+1}-1$. Dacă u nu este prim, avînd $\nu\geqslant 1$, avem $2^{\nu+1}-1>1$, deci printre divizorii pozitivi ai lui u figurează $2^{\nu+1}-1$, 1 și încă alți divizori pozitivi ai lui u. Dar atunci $\sigma(u)=\sum\limits_{d|u} d>(2^{\nu+1}-1)+1=2^{\nu+1}$ ceea ce contrazice $\sigma(u)=2^{\nu+1}$. Deci dacă numărul natural par n este perfect, el este de forma $n=2^{\nu}(2^{\nu+1}-1)$, unde $\nu\geqslant 1$, iar $2^{\nu+1}-1$ este prim.

Condiția este suficientă. Dacă numărul natural n par se scrie sub forma $n=2^{\nu}(2^{\nu+1}-1)$ unde $\nu\geqslant 1$, iar $2^{\nu+1}-1$ este prim, avem $(2^{\nu}, 2^{\nu+1}-1)\cong 1$, numărul $2^{\nu+1}-1$ fiind impar, deci, funcția σ fiind multiplicativă

$$\sigma(n)=\sigma(2^{\nu}(2^{\nu+1}-1))=\sigma(2^{\nu})\ \sigma(2^{\nu+1}-1)=$$

$$=\Big(\sum_{\delta=0}^{\nu} 2^{\delta}\Big)((2^{\nu+1}-1)+1)=\frac{2^{\nu+1}-1}{2-1}2^{\nu+1}=2^{\nu+1}(2^{\nu+1}-1)=2n,$$

deci numărul natural n par considerat este perfect.

Observație. Demonstrația suficienței a fost dată de Euclid, iar demonstrația necesității a fost dată de Euler, după ce au trecut aproape 2 000 de ani de la demonstrația suficienței.

Nu toate numerele impare de forma $2^{\nu+1}-1$, unde ν este un număr natural, sînt prime. Pentru $\nu=1$ și $\nu=2$ obținem respectiv numere prime $2^{1+1}-1=2^2-1=3$ și $2^{2+1}-1=2^3-1=7$. Pentru $\nu=3$ numărul $2^{3+1}-1=2^4-1=15$ nu mai este prim. Deci $n=2^1\cdot 3=6$ și $n=2^2\cdot 7=28$ sînt numere naturale pare perfecte.

Teoremă. *O condiție necesară ca numerele de forma* $2^{\nu+1}-1$, *unde* ν *este un număr natural, să fie prime este ca* $\nu+1$ *să fie prim.*

Demonstrație. Dacă $\nu+1$ nu este prim, el se scrie sub forma unui produs $\alpha\beta$, unde $\alpha>1$ și $\beta>1$ și atunci

$2^{\nu+1}-1=2^{\alpha\beta}-1=(2^\alpha-1)(2^{\alpha(\beta-1)}+2^{\alpha(\beta-2)}+\ldots+2^\alpha+1)$, deci $2^{\nu+1}-1$ nu este prim avînd $2^\alpha-1>1$, $2^{\alpha(\beta-1)}+2^{\alpha(\beta-2)}+\ldots+2^\alpha+1>1$.

Dacă $\nu+1$ este prim nu rezultă că neapărat $2^{\nu+1}-1$ este prim. De exemplu, pentru $\nu+1=11$ avem $2^{11}-1=2\,047=23\cdot 89$, deci $2^{11}-1$ nu este prim.

Numere prime ale lui Mersenne. *Numerele de forma* $2^\pi-1$, *care sînt prime atunci cînd* π *este un număr prim pozitiv, se numesc numere prime ale lui Mersenne.*

Nu se știe dacă există o infinitate de numere prime ale lui Mersenne.

Cu ajutorul numerelor prime ale lui Mersenne, numerele perfecte se scriu sub forma

$$2^{\pi-1}p,$$

unde π este un număr prim pozitiv astfel încît $p=2^\pi-1$ să fie un număr prim al lui Mersenne.

Pînă acum nu se cunoaște nici un număr natural impar care să fie perfect.

Dacă ne referim la numărul divizorilor primi pozitivi distincți doi cîte doi ai unui număr natural perfect, constatăm că acest număr trebuie să fie cel puțin egal cu 2, deoarece dacă $n=p^\alpha$, unde p este un număr prim pozitiv, iar α este un număr natural, atunci

$$\sigma(n)=1+p+\ldots+p^{\alpha-1}+p^\alpha=\frac{p^{\alpha+1}-1}{p-1}<p^\alpha\frac{p}{p-1}\leqslant 2p^\alpha,$$

fiindcă din $2\leqslant p$ rezultă $p\leqslant 2p-2$ sau $\frac{p}{p-1}\leqslant 2$, avînd $p-1>0$, deoarece $p-1\geqslant 1$, deci $\sigma(n)<2n$.

În cazul numerelor perfecte naturale pare, numărul divizorilor primi pozitivi diferiți doi cîte doi ai acestor numere este egal *numai cu doi*, cum se vede din teorema precedentă.

În cazul numerelor perfecte naturale impare, numărul divizorilor primi pozitivi diferiți doi cîte doi ai acestor numere este egal cel puțin cu trei, deoarece dacă $n=p_1^{\alpha_1}p_2^{\alpha_2}$ unde p_1 și p_2 sînt numere prime pozitive diferite, iar α_1 și α_2 sînt numere naturale, avem $p_1\geqslant 3$, $p_2\geqslant 5$ și

$$\sigma(n)=\sigma(p_1^{\alpha_1})\ \sigma(p_2^{\alpha_2})=\frac{p_1^{\alpha_1+1}-1}{p_1-1}\ \frac{p_2^{\alpha_2+1}-1}{p_2-1}<p_1^{\alpha_1}p_2^{\alpha_2}\ \frac{p_1}{p_1-1}\ \frac{p_2}{p_2-1}\leqslant$$

$$\leqslant n\,\frac{3}{2}\,\frac{5}{4}<2n,$$

fiindcă din $3\leqslant p_1$ și $5\leqslant p_2$ rezultă $2p_1\leqslant 3(p_1-1)$ și $4p_2\leqslant 5(p_2-1)$ sau $\frac{p_1}{p_1-1}\leqslant\frac{3}{2}$ și $\frac{p_2}{p_2-1}\leqslant\frac{5}{4}$, avînd $p_1-1>0$ și $p_2-1>0$, deci $\sigma(n)<2n$.

O altă condiție necesară ca un număr natural impar să fie perfect este dată de următoarea:

Teoremă. *Un număr natural impar* n *poate fi perfect numai dacă*

$$n=p_1^{\alpha_1}p_2^{\alpha_2}\ldots\ p_r^{\alpha_r},$$

în care $p_1, p_2, \ldots, p_r$ *sînt numere prime impare,* $0<p_1<p_2<\ldots<p_r$, *iar* $\alpha_1, \alpha_2, \ldots, \alpha_r$ *sînt numere naturale, și există un număr natural* i, $i\neq 1$, *numere naturale* $k_1, k_2, \ldots, k_{i-1}, k_{i+1}, \ldots, k_r$ *și un număr întreg nenegativ* k_i *astfel încît să avem* $\alpha_1=2k_1, \ldots, \alpha_{i-1}=2k_{i-1}, \alpha_i=4k_i+1, \alpha_{i+1}=2k_{i+1}, \ldots, \alpha_r=2k_r$ *și* $p_i\equiv 1 \pmod 4$.

Demonstrație.

$$\sigma(n)=\sigma(p_1^{\alpha_1})\ldots\sigma(p_r^{\alpha_r})=(1+p_1+\ldots+p_1^{\alpha_1})\ldots(1+p_r+\ldots$$

$$\ldots+p_r^{\alpha_r}).$$

Dacă α_i este impar atunci

$$1+p_i+\ldots+p_i^{\alpha_i}\equiv 0 \pmod 2.$$

Deci ca să putem avea $\sigma(n)=2n$ trebuie ca într-o singură paranteză să avem $\alpha_i\not\equiv 0 \pmod 2$, iar pentru toate celelalte paranteze trebuie ca $\alpha_i\equiv 0 \pmod 2$.

În cazul $\alpha_i \not\equiv 0 \pmod 2$ nu putem avea $\alpha_i \equiv 3 \pmod 4$, deoarece în acest caz $\alpha_i = 4k+3$ și $1+p_i+\ldots+p_i^{\alpha_i} = \frac{p_i^{\alpha_i+1}-1}{p_i-1} =$

$$= \frac{p_i^{4k+4}-1}{p_i-1} = \frac{(p_i^{4k+2}+1)(p_i^{4k+2}-1)}{p_i-1} = (p_i^{4k+2}+1)(p_i^{4k+1}+p_i^{4k}+\ldots$$

$\ldots+p_i+1) \equiv 0 \pmod 4$, ceea ce vine în contrazicere cu $\sigma(n) \not\equiv 0 \pmod 4$. Deci trebuie să considerăm că $\alpha_i \equiv 1 \pmod 4$. Atunci

$$1+p_i+\ldots+p_i^{\alpha_i} = \frac{p_i^{\alpha_i+1}-1}{p_i-1} = \frac{p_i^{4k+2}-1}{p_i-1} = \frac{(p_i^{2k+1}+1)(p_i^{2k+1}-1)}{p_i-1} =$$

$$=(p_i+1)(1-p_i+p_i^2-\ldots+p_i^{2k})(1+p_i+p_i^2+\ldots+p_i^{2k}).$$

Deoarece $\sigma(n) \equiv 0 \pmod 2$, dar $\sigma(n) \not\equiv 0 \pmod 4$, trebuie ca $p_i+1 \equiv 0 \pmod 2$, dar $p_i+1 \not\equiv 0 \pmod 4$. Nu putem avea $p_i+1 \equiv 1 \pmod 4$ și nici $p_i+1 \equiv 3 \pmod 4$, deoarece $p_i+1 \equiv 0 \pmod 2$. Așadar trebuie să avem $p_i+1 \equiv 2 \pmod 4$. Deci $p_i \equiv 1 \pmod 4$. Avem $p_i+1=2s$ cu $s \neq 1$, pentru că $p_i \neq 1$ și $s=p_j t$ cu p_j unul dintre $p_1, \ldots, p_{i-1}, p_{i+1}, \ldots p_r$ din cauză că

$$\sigma(n)=\sigma(p_1^{\alpha_1})\ldots\sigma(p_{i-1}^{\alpha_{i-1}})(p_i+1)(1-p_i+p_i^2-\ldots+p_i^{2k_i})(1+p_i+$$

$$+p_i^2+\ldots+p_i^{2k_i})\sigma(p_{i+1}^{\alpha_{i+1}})\ldots\sigma(p_r^{\alpha_r})=$$

$$=2p_1^{2k_1}\ldots p_{i-1}^{2k_{i-1}}\ p_i^{4k_i+1}p_{i+1}^{2k_{i+1}}\ldots p_r^{2k_r}.$$

Dacă $i=1$ atunci $p_i<p_j$ $(j \neq 1)$ și deci $p_i+1<p_j+1$ sau $2p_jt<$ $<p_j+1$ din cauză că $p_i+1=2s=2p_jt$. Deci $p_j(2t-1)<1$, ceea ce nu se poate, deoarece $p_j>1$ și $2t-1 \geqslant 1$. Deci $i \neq 1$ și cu aceasta teorema este demonstrată.

Numere prime ale lui Fermat. Tot atît de celebre ca numerele prime ale lui Mersenne, poate chiar mai celebre, sînt numerele prime ale lui Fermat.

Numerele de forma $2^{2^n}+1$ care sînt prime atunci cînd n este un număr natural sau zero se numesc numere prime ale lui Fermat.

Nu se știe dacă există o infinitate de numere prime ale lui Fermat.

Pentru $n=0, 1, 2, 3, 4$ obținem numere prime 3, 5, 17, 257, 65537, dar pentru $n=5$ numărul $2^{2^5}+1$ se divide cu 641, după cum a arătat Euler prin metoda din 1.4, exemplul 2.

Celebritatea numerelor prime ale lui Fermat constă în faptul demonstrat de Gauss că un poligon regulat cu n laturi poate fi construit numai cu rigla și compasul, dacă și numai dacă avem

$$n=2^{\alpha}p_1\ldots p_r,$$

unde α este un număr întreg nenegativ, iar $p_1, \ldots, p_r$ sînt numere prime ale lui Fermat.

Capitolul 8

FORMULE DE INVERSARE A SUMELOR

8.1. Funcția lui Moebius

În formulele de inversare a sumelor un rol important îl joacă funcția lui Moebius.

Definiție. *Funcția lui Moebius notată cu* μ *este o funcție numerică care are următoarele valori :*

$$\mu(n)=\begin{cases}(-1)^k & \text{dacă nu există nici un număr prim } p \text{ astfel încît } p^2|n, \text{ iar } k \text{ este numărul tuturor numerelor prime } p_1, p_2, \ldots, p_k \text{ neasociate două cîte două astfel încît } p_1|n, \ldots, p_k|n.\\ 0 & \text{dacă există un număr prim } p \text{ astfel încît } p^2|n.\end{cases}$$

Exemple.

$\mu(12)=\mu(2^2 3)=0$, $\mu(15)=\mu(3\cdot 5)=(-1)^2=1$, $\mu(30)=\mu(2\cdot 3\cdot 5)=$ $=(-1)^3=-1$.

Teoremă. *Funcția lui Moebius este multiplicativă.*

Demonstrație. Dacă $(m, n)\cong 1$ și $m\neq 0$, $n\neq 0$, atunci $m=\varepsilon_m p_1^{\alpha_1}\cdot p_2^{\alpha_2}\ldots p_r^{\alpha_r}$, $n=\varepsilon_m p_{r+1}^{\alpha_{r+1}} p_{r+2}^{\alpha_{r+2}}\ldots p_s^{\alpha_s}$, unde $\alpha_1, \alpha_2, \ldots, \alpha_r, \alpha_{r+1}, \alpha_{r+2}, \ldots, \alpha_s$ sînt numere naturale, $\varepsilon_m=\pm 1$, $\varepsilon_n=\pm 1$, iar $p_1, p_2, \ldots, p_r, p_{r+1}, p_{r+2}, \ldots, p_s$ sînt numere prime neasociate două cîte două, deoarece dacă două din aceste numere prime ar fi asociate atunci sau în m sau în n numerele prime nu sînt neasociate două cîte două, contrar modului de scriere a numerelor m și n, sau valoarea p a unuia dintre ele ar divide și pe m și pe n deci și pe 1, deoarece $(m, n)\cong 1$, deci $p|1$, ceea ce este absurd, p fiind prim. Avem deci

$$mn=\varepsilon_m\varepsilon_n p_1^{\alpha_1} p_2^{\alpha_2}\ldots p_r^{\alpha_r} p_{r+1}^{\alpha_{r+1}} p_{r+2}^{\alpha_{r+2}}\ldots p_s^{\alpha_s}.$$

Dacă $\alpha_1=\alpha_2=\ldots=\alpha_r=\alpha_{r+1}=\alpha_{r+2}=\ldots=\alpha_s=1$, atunci

$$\mu(m)=(-1)^r,\quad \mu(n)=(-1)^{s-r},\quad \mu(mn)=(-1)^s$$

și deci $\mu(mn)=\mu(m)\,\mu(n)$. Dacă cel puțin unul dintre $\alpha_1, \alpha_2, \ldots, \alpha_r, \alpha_{r+1}, \alpha_{r+2}, \ldots, \alpha_s$ este mai mare ca 1, atunci $\mu(mn)=0$ și cel puțin unul dintre $\mu(m)$, $\mu(n)$ este egal cu zero, deci și în acest caz

$$\mu(mn)=\mu(m)\,\mu(n).$$

Același lucru se întîmplă și în cazul cînd cel puțin unul dintre m și n este egal cu zero. Cu aceasta teorema este demonstrată.

Teoremă. *Funcția de sumare a funcției lui Moebius este*

$$\sum_{d|n}\mu(d)=\begin{cases}1 & \text{dacă } n=\pm 1,\\ 0 & \text{în toate celelalte cazuri.}\end{cases}$$

Demonstrație. Dacă $n=\pm 1$ avem

$$\sum_{d|\pm 1}\mu(d)=\mu(1)=1,$$

pentru că nu există nici un număr prim p astfel încît $p^2|1$ și, pentru că nu există nici un număr prim p astfel încît $p|1$, deci $k=0$ și $\mu(1)=(-1)^0=1$.

Dacă $n=0$, prin definiție

$$\sum_{d|0}\mu(d)=0.$$

Dacă $n\neq 0$, $n\neq\pm 1$ avem $n=\pm p_1^{\alpha_1} p_2^{\alpha_2}\ldots p_r^{\alpha_r}$. Vom pune $a=p_1^{\alpha_1}$ și $b=\pm p_2^{\alpha_2}\ldots p_r^{\alpha_r}$. Avem $(a, b)\cong 1$, pentru că $p_1, p_2, \ldots, p_r$ sînt

numere prime neasociate două cîte două. Deoarece $\alpha_1, \alpha_2, \ldots, \alpha_r$ sînt numere naturale, iar funcția lui Moebius este multiplicativă avem

$$\sum_{d|n}\mu(d)=\left(\sum_{d_1|a}\mu(d_1)\right)\left(\sum_{d_2|b}\mu(d_2)\right)=\left(\sum_{\delta_1=0}^{\alpha_1}\mu(p_1^{\delta_1})\right)\left(\sum_{d_2|b}\mu(d_2)\right)=\left(\mu(p_1^0)+\right.$$

$$\left.+\mu(p_1)+\mu(p_1^2)+\ldots+\mu(p_1^{\alpha_1})\right)\left(\sum_{d_2|b}\mu(d_2)\right)=\left((-1)^0+(-1)^1+\right.$$

$$\left.\underbrace{+0+\ldots+0}_{de\ \alpha_1-1\ ori}\right)\left(\sum_{d_2|b}\mu(d_2)\right)=(1-1)\sum_{d_2|b}\mu(d_2)=0.$$

8.2. Formula de inversare a lui Moebius

Înainte de a da această formulă, vom da cîteva moduri de schimbare a ordinii de sumare în funcția de sumare a funcțiilor numerice.

Teoremă. *Avem*

$$\sum_{d|n}\left(\sum_{c\left|\frac{n}{d}\right.}g(d,\ c)\right)=\sum_{c|n}\left(\sum_{d\left|\frac{n}{c}\right.}g(d,\ c)\right).$$

Demonstrație. Notăm cu M mulțimea tuturor perechilor $(d,\ c)$ astfel încît $d>0,\ c>0,\ d|n,\ c\left|\frac{n}{d}\right.$, $M=\left\{(d,\ c)\mid d>0\&c>0\&d|n\&\right.$ $\left.\&c\left|\frac{n}{d}\right.\right\}$ și cu N mulțimea tuturor perechilor $(d,\ c)$ astfel încît $d>0,\ c>0,\ c|n,\ d\left|\frac{n}{c}\right.$, $N=\left\{(d,\ c)\mid d>0\&c>0\&c|n\&d\left|\frac{n}{c}\right.\right\}$. Vom arăta că $M=N$.

Într-adevăr, fie $(d,\ c)\in M$. Atunci $d>0,\ c>0,\ d|n,\ c\left|\frac{n}{d}\right.$. Din $c\left|\frac{n}{d}\right.$ rezultă $c\left|\frac{n}{d}d\right.$, deci $c|n$. Apoi tot din $c\left|\frac{n}{d}\right.$ deducem $dc\left|\frac{n}{d}d\right.$, deci $dc|n$. Însă am arătat că $c|n$ și cum $c>0$, rezultă că $c\neq 0$ și că $\frac{n}{c}$ este un număr întreg, deci din $dc|n$ deducem $d\left|\frac{n}{c}\right.$. Cu

aceasta am arătat că $(d,\ c)\in N$, deci $M\subseteq N$. Demonstrația faptului că $N\subseteq M$ se obține schimbînd în demonstrația precedentă pe d cu c și pe c cu d. Deci $M=N$.

Perechile de numere $(d,\ c)$ după care se face suma $\sum_{d|n}\left(\sum_{c\left|\frac{n}{d}\right.}g(d,\ c)\right)$ formează mulțimea M și fiecare din ele apare o singură dată în suma considerată, conform cu modul în care a fost definită suma considerată. Perechile de numere $(d,\ c)$ după care se face suma $\sum_{c|n}\left(\sum_{d\left|\frac{n}{c}\right.}g(d,\ c)\right)$ formează mulțimea N și fiecare din ele apare o singură dată în suma considerată, conform cu modul în care a fost definită suma considerată. Deoarece mulțimile M și N sînt egale, sînt egale și cele două sume considerate.

Teoremă.

$$\sum_{d|n}\left(\sum_{c|d}g\left(\frac{d}{c},\ c\right)\right)=\sum_{c|n}\left(\sum_{h\left|\frac{n}{c}\right.}g(h,c)\right)$$

Demonstrație. Notăm cu M mulțimea tuturor perechilor $\left(\frac{d}{c},\ c\right)$ astfel încît $d>0,\ c>0,\ d|n,\ c|d,\ M=\left\{\left(\frac{d}{c},\ c\right)\right.\mid d>0\&c>0\&d|n\&$ $\left.\&c|d\right\}$ și cu N mulțimea tuturor perechilor $(h,\ c)$ astfel încît $h>0,$ $c>0,\ h\left|\frac{n}{c}\right.,\ c|n,\ N=\left\{(h,\ c)\mid h>0\&c>0\&h\left|\frac{n}{c}\right.\&c|n\right\}$. Vom arăta că $M=N$.

Într-adevăr, fie $\left(\frac{d}{c},\ c\right)\in M$. Atunci $d>0,\ c>0\ d|n,\ c|d$. Din $c>0$ rezultă că $c\neq 0$ și deci din $c|d$ rezultă că $\frac{d}{c}$ este un număr întreg. Din $c|d$ și $d|n$ rezultă $c|n$. Ținînd seama de $c\neq 0$, din $c|n$ rezultă că $\frac{n}{c}$ este un număr întreg. Cum $c\neq 0$ și $d|n$ rezultă $\frac{d}{c}\left|\frac{n}{c}\right.$ $\frac{d}{c}$ și $\frac{n}{c}$ fiind numere întregi, unde $\frac{d}{c}>0$, avînd $d>0,\ c>0$. Deoarece și $c|n,\ c>0$ rezultă că $\left(\frac{d}{c},\ c\right)\in N$, deci $M\subseteq N$. Fie acum $(h,\ c)\in N$. Atunci $h>0, c>0, h\left|\frac{n}{c}\right.,\ c|n$. Din $h\left|\frac{n}{c}\right.$ obținem $hc\left|\frac{n}{c}c\right.$

deci $hc|n$. Dacă notăm $d=hc$ obținem $d>0$, ca urmare a faptului că $h>0$, $c>0$ și apoi $d|n$, deoarece $hc|n$. Mai avem și $c|d$, deoarece $d=hc$, la care se adaugă $c>0$. Deci $(h, c)\in M$. Așadar, am dovedit că $M=N$.

Perechile de numere $\left(\frac{d}{c}, c\right)$ după care se face suma $\sum_{d|n}\left(\sum_{c|d} g\left(\frac{d}{c}, c\right)\right)$ formează mulțimea M și fiecare din ele apare o singură dată în suma considerată, conform cu modul în care a fost definită suma considerată. Perechile de numere (h, c) după care se face suma $\sum_{c|n}\left(\sum_{h\left|\frac{n}{c}\right.} g(h, c)\right)$ formează mulțimea N și fiecare din ele apare o singură dată în suma considerată, conform cu modul în care a fost definită suma considerată. Deoarece mulțimile M și N sînt egale, sînt egale și cele două sume considerate.

Consecință.

$$\sum_{d|n}\sum_{c|d} g\left(\frac{d}{c}, c\right)=\sum_{h|n}\sum_{c\left|\frac{n}{h}\right.} g(h, c).$$

Formula de inversare a lui Moebius constă în următoarea teoremă.

Teoremă. *Dacă f este o funcție numerică astfel încît $f(n)=f(-n)$ oricare ar fi numărul întreg n atunci din*

$$F(n)=\sum_{d|n} f(d)$$

rezultă

$$f(n)=\sum_{d|n}\mu(d)\, F\left(\frac{n}{d}\right)$$

și reciproc dacă F este o funcție numerică astfel încît $F(n)=F(-n)$ oricare ar fi numărul întreg n. Se consideră $n\neq 0$.

Demonstrație. Dacă

$$F(n)=\sum_{d|n} f(d)$$

atunci

$$\sum_{d|n}\mu(d)\, F\left(\frac{n}{d}\right)=\sum_{d|n}\mu(d)\left(\sum_{c\left|\frac{n}{d}\right.} f(c)\right)=\sum_{d|n}\left(\sum_{c\left|\frac{n}{d}\right.}\mu(d)\, f(c)\right)=$$
$$=\sum_{c|n}\left(\sum_{d\left|\frac{n}{c}\right.}\mu(d)\, f(c)\right)=\sum_{c|n} f(c)\left(\sum_{d\left|\frac{n}{c}\right.}\mu(d)\right)=f(n),$$

deoarece, atîta timp cît $\frac{n}{c}\neq\pm 1$, adică $c\neq\pm n$, avem $\sum_{d\left|\frac{n}{c}\right.}\mu(d)=0$ și numai pentru $c=\pm n$ avem $\sum_{d\left|\frac{n}{c}\right.}\mu(d)=1$. Am ținut seama și de $f(n)=f(-n)$, deoarece avînd $0<c$ trebuie ca $c=n$ dacă $n>0$ și $c=-n$ dacă $n<0$.

Reciproc, dacă

$$f(n)=\sum_{d|n}\mu(d)\, F\left(\frac{n}{d}\right)$$

atunci

$$\sum_{d|n} f(d)=\sum_{d|n}\left(\sum_{c|d}\mu(c)\, F\left(\frac{d}{c}\right)\right)=\sum_{c|n}\left(\sum_{h\left|\frac{n}{c}\right.}\mu(c)\, F(h)\right)=$$
$$=\sum_{h|n}\left(\sum_{c\left|\frac{n}{h}\right.}\mu(c)\, F(h)\right)=\sum_{h|n} F(h)\left(\sum_{c\left|\frac{n}{h}\right.}\mu(c)\right)=F(n),$$

deoarece, atîta timp cît $\frac{n}{h}\neq\pm 1$, adică $h\neq\pm n$, avem $\sum_{c\left|\frac{n}{h}\right.}\mu(c)=0$ și numai pentru $h=\pm n$ avem $\sum_{c\left|\frac{n}{h}\right.}\mu(c)=1$. Am ținut seama și de $F(n)=F(-n)$, deoarece avînd $0<h$ trebuie ca $h=n$ dacă $n>0$ și $h=-n$ dacă $n<0$.

O aplicație a formulei de inversare a lui Moebius este următoarea:

Teoremă. *Dacă funcția de sumare a unei funcții numerice f este total-multiplicativă sau numai multiplicativă, atunci funcția f este multiplicativă, cu condiția ca $f(0)=0$ sau $f(0)=1$, dar în ultimul caz $f(\pm 1)=1$.*

Demonstrație. Avem

$$F(a)=\sum_{d|a} f(d)$$

în cazul cînd $a\neq 0$. Atunci

$$f(a)=\sum_{d|a}\mu(d)\, F\left(\frac{a}{d}\right).$$

Dacă pe lîngă $a\neq 0$ mai avem $a=mn$ și $(m,\ n)\cong 1$, atunci

$$f(mn)=\sum_{d|mn}\mu(d)\,F\left(\frac{mn}{d}\right)=\sum_{d_1|m}\left(\sum_{d_2|n}\mu(d_1d_2)\,F\left(\frac{mn}{d_1d_2}\right)\right).$$

Din $d_1|m$, $d_2|n$ și $(m,\ n)\cong 1$ rezultă $(d_1,\ d_2)\cong 1$ scriind $m=d_1m_1$, $n=d_2n_2$, deci $(d_1m_1,\ d_2n_2)\cong 1$, deci $(d_1,\ d_2n_2)\cong 1$, deci $(d_1,\ d_2)\cong 1$. Rezultă că $\mu(d_1d_2)=\mu(d_1)\,\mu(d_2)$, funcția lui Moebius fiind multiplicativă. Dacă funcția F este total-multiplicativă, putem scrie

$$F\left(\frac{mn}{d_1d_2}\right)=F\left(\frac{m}{d_1}\right)F\left(\frac{n}{d_2}\right),$$

$\frac{m}{d_1}$ și $\frac{m}{d_2}$ fiind numere întregi. Același lucru putem scrie și dacă funcția F este multiplicativă, deoarece, cu notațiile de mai sus $\frac{m}{d_1}=m_1$, $\frac{n}{d_2}=n_2$ și din $(m,\ n)\cong 1$ rezultă $(m_1d_1,\ n_2d_2)\cong 1$, deci $(m_1,\ n_2d_2)\cong 1$, deci $(m_1,\ n_2)\cong 1$, deci $\left(\frac{m}{d_1},\ \frac{n}{d_2}\right)\cong 1$. Așadar

$$f(mn)=\sum_{d_1|m}\left(\sum_{d_2|n}\mu(d_1)\,\mu(d_2)\,F\left(\frac{m}{d_1}\right)F\left(\frac{n}{d_2}\right)\right)=$$

$$=\sum_{d_1|m}\mu(d_1)\,F\left(\frac{m}{d_1}\right)\left(\sum_{d_2|n}\mu(d_2)\,F\left(\frac{n}{d_2}\right)\right)=$$

$$=\left(\sum_{d_1|m}\mu(d_1)\,F\left(\frac{m}{d_1}\right)\right)\left(\sum_{d_2|n}\mu(d_2)\,F\left(\frac{n}{d_2}\right)\right)=f(m)\,f(n).$$

În cazul cînd $a=0$, $a=mn$ și $(m,\ n)\cong 1$, atunci sau $m=0$, $n=\pm 1$ sau $m=\pm 1$, $n=0$. Dacă $f(0)=0$ atunci

$$0=f(0)=f(0)\,f(\pm 1)=0f(\pm 1),$$
$$0=f(0)=f(\pm 1)\,f(0)=f(\pm 1)0.$$

Dacă $f(0)=1$ atunci

$$1=f(0)=f(0)\,f(\pm 1)=1\cdot 1,$$
$$1=f(0)=f(\pm 1)\,f(0)=1\cdot 1,$$

deoarece $f(\pm 1)=1$.

O altă aplicație a formulei de inversare a lui Moebius este stabilirea formulei de calcul pentru funcția lui Euler. În acest scop, mai întîi, trebuie să arătăm că $\sum_{d|n}\varphi(d)=|n|$ dacă $n\neq 0$. Mai întîi însă, vom stabili următoarea:

Teoremă. *Avem*

$$\sum_{d|n}g\left(\frac{|n|}{d}\right)=\sum_{h|n}g(h),$$

g fiind o funcție numerică.

Demonstrație. Notăm cu M mulțimea tuturor numerelor de forma $\frac{|n|}{d}$, unde $d|n$ și $d>0$, $M=\left\{\frac{|n|}{d}\;\middle|\;d>0\,\&\,d|n\right\}$, și cu N notăm mulțimea tuturor divizorilor pozitivi ai lui n, $N=\{h|\ h>0\,\&\,\&\,h|n\}$. Avem $M=N$.

Într-adevăr, fie $\frac{|n|}{d}\in M$. Atunci $d|n$ și $d>0$ deci $d||n|$ și adăugînd $d>0$ rezultă că $\frac{|n|}{d}$ este număr întreg. Deci $\frac{|n|}{d}\,\Big|\,\frac{|n|}{d}$, deci $\frac{|n|}{d}\,\Big|\,\frac{|n|}{d}\,d$ sign n, deci $\frac{|n|}{d}\,\Big|\,n$. Luînd $h=\frac{|n|}{d}$ rezultă $h\in N$, deoarece $\frac{|n|}{d}>0$. Am arătat deci că $M\subseteq N$. Fie acum $h\in N$. Atunci $h|n$ și $h>0$. Deci $h||n|$, deci există un număr întreg d astfel încît $|n|=hd$. Deoarece $|n|>0$, $h>0$ avem și $d>0$. Apoi din $|n|=hd$ rezultă $d||n|$, deci $d|n$. Așadar, $h=\frac{|n|}{d}$ cu $d>0$ și $d|n$, deci $h\in M$. Am arătat deci că $N\subseteq M$ și deci avem $M=N$.

Numerele $\frac{|n|}{d}$ după care se face suma $\sum_{d|n}g\left(\frac{|n|}{d}\right)$ formează mulțimea M și fiecare din ele apare o singură dată în suma considerată, conform cu modul în care este definită această sumă. Numerele h după care se face suma $\sum_{h|n}g(h)$ formează mulțimea N și fiecare din ele apare o singură dată în suma considerată, conform cu modul în care este definită această sumă. Mulțimile M și N fiind egale, sînt egale și cele două sume considerate.

Teoremă. *Dacă $n\neq 0$, atunci*

$$\sum_{d|n}\varphi(d)=|n|.$$

Demonstrație. Considerăm toate clasele de resturi modulo n. Deoarece $n\neq 0$, numărul claselor de resturi modulo n este egal cu $|n|$.

Să determinăm, acum, numărul claselor de resturi modulo n și prin următorul procedeu. Considerăm o clasă de resturi C_a modulo n și luăm $d \cong (a, n)$. Dacă schimbăm reprezentantul acestei clase, deci dacă luăm $C_b = C_a$ atunci $(b, n) \cong d$, conform proprietății (8, a) din 1.2 a relației de congruență. Deci fiecărei clase de resturi C_a modulo n îi corespunde un singur divizor pozitiv d al lui n astfel încît $(a, n) \cong d$. Putem lua pe d pozitiv datorită proprietății de unicitate a celui mai mare divizor comun a două numere întregi, avînd $n \neq 0$. Reciproc, pentru fiecare divizor pozitiv d al lui n există o clasă de resturi modulo n anume C_d astfel încît $(d, n) \cong d$. Să numărăm acum clasele de resturi C_a modulo n care corespund unui divizor pozitiv d al lui n, astfel încît $(a, n) \cong d$. Acest lucru se face în felul următor. Fiind dată o clasă de resturi C_a modulo n astfel încît $(a, n) \cong d$ obținem $a = da_1$, $n = dn_1$, $(a_1, n_1) \cong 1$, deoarece $n \neq 0$. Deci la fiecare clasă de resturi C_a modulo n cu $(a, n) \cong d$ îi corespunde o clasă de resturi C_{a_1} primă cu modulul n_1 și îi corespunde o singură astfel de clasă, deoarece luînd $C_b = C_a$ obținem $b \equiv a \pmod n$, deci $b_1 \equiv a_1 \pmod{n_1}$ unde $b = db_1$, deci $C_{b_1} = C_{a_1}$. Reciproc fiecărei clase de resturi C_{a_1} modulo n_1 primă cu modulul îi corespunde o clasă de resturi C_a modulo n astfel încît $a = da_1$ și $(a, n) \cong d$ și îi corespunde o singură astfel de clasă, deoarece din $C_{b_1} = C_{a_1}$ obținem $b_1 \equiv a_1 \pmod{n_1}$, deci $b \equiv a \pmod n$, iar $(b, n) \cong (a, n) \cong d$. Deci numărul claselor de resturi C_a modulo n, unde $(a, n) \cong d$, este egal cu numărul claselor de resturi C_{a_1} modulo n_1 prime cu modulul, unde $a = da_1$, $n = dn_1$. Acest ultim număr este egal cu $\varphi(n_1) = \varphi(n : d) = \varphi\left(\frac{n}{d}\right)$. Adunînd toate aceste numere, adică făcînd suma $\sum_{d|n} \varphi\left(\frac{n}{d}\right)$, obținem numărul claselor de resturi modulo n, deci

$$\sum_{d|n} \varphi\left(\frac{n}{d}\right) = |n|.$$

Deoarece $\varphi\left(\frac{n}{d}\right) = \varphi\left(\frac{|n|}{d}\right)$, putem scrie $\sum_{d|n} \varphi\left(\frac{n}{d}\right) = \sum_{d|n} \varphi\left(\frac{|n|}{d}\right)$. Însă $\sum_{d|n} \varphi\left(\frac{|n|}{d}\right) = \sum_{h|n} \varphi(h)$. Schimbînd notațiile pentru a apare d în locul lui h obținem

$$\sum_{d|n} \varphi(d) = |n|.$$

Observație. Relația $\sum_{d|n} \varphi(d) = |n|$ pentru $n \neq 0$ poate fi demonstrată și în felul următor. Dacă $n = \pm 1$, atunci $\sum_{d|\pm 1} \varphi(d) = \varphi(1) = 1 = |\pm 1|$. Dacă $n \neq \pm 1$, cum avem și $n \neq 0$ putem scrie $n = \pm p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots p_r^{\alpha_r}$, unde $p_1, p_2, \ldots, p_r$ sînt numere prime pozitive diferite două cîte două, iar $\alpha_1, \alpha_2, \ldots, \alpha_r$ sînt numere naturale. Luînd $a = p_1^{\alpha_1}$, $b = \pm p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ constatăm că $(a, b) \cong 1$, pentru că $p_1, p_2 \ldots, \ldots, p_r$ sînt numere prime pozitive diferite două cîte două. Deoarece funcția lui Euler este multiplicativă obținem

$$\sum_{d|n} \varphi(d) = \left(\sum_{d_1|a} \varphi(d_1)\right)\left(\sum_{d_2|b} \varphi(d_2)\right) = \left(\sum_{\delta_1=0}^{\alpha_1} \varphi(p_1^{\delta_1})\right)\left(\sum_{d_2|b} \varphi(d_2)\right) = (\varphi(p_1^0) + \varphi(p_1) + \varphi(p_1^2) + \ldots + \varphi(p_1^{\alpha_1}))\left(\sum_{d_2|b} \varphi(d_2)\right) = (1 + p_1 - 1 + p_1^2 - p_1 + \ldots + p_1^{\alpha_1} - p_1^{\alpha_1 - 1})\left(\sum_{d_2|b} \varphi(d_2)\right) = p_1^{\alpha_1}\left(\sum_{d_2|b} \varphi(d_2)\right).$$

Repetînd procedeul, ajungem în cele din urmă la

$$\sum_{d|n} \varphi(d) = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r} = |n|.$$

Spre deosebire de prima demonstrație, în cea de a doua demonstrație am ținut seama de faptul că funcția lui Euler este multiplicativă și am utilizat formulele de calcul $\varphi(p_1^0) = \varphi(1) = 1$, $\varphi(p_1^{\delta_1}) = p_1^{\delta_1} - p_1^{\delta_1 - 1}$ în cazul cînd p_1 este număr prim pozitiv, iar δ_1 este un număr natural.

Utilizînd, acum, formula de inversare a lui Moebius obținem următoarea formulă de calcul a funcției lui Euler.

Teoremă. *Avem*

$$\varphi(n) = |n| \sum_{d|n} \frac{\mu(d)}{d}.$$

Demonstrație. Avem $\sum_{d|n} \varphi(d) = |n|$ și $\varphi(n) = \varphi(-n)$ oricare ar fi numărul întreg n. Formula de inversare a lui Moebius ne dă $\varphi(n) = \sum_{d|n} \mu(d) \left|\frac{n}{d}\right|$. Deci $\varphi(n) = \sum_{d|n} \mu(d) \frac{|n|}{d}$ de unde $\varphi(n) = |n| \sum_{d|n} \frac{\mu(d)}{d}$.

De la această formulă de calcul se trece la formula de calcul

$$\varphi(n) = p_1^{\alpha_1 - 1} \; p_2^{\alpha_2 - 1} \ldots \; p_r^{\alpha_r - 1} (p_1 - 1)(p_2 - 1) \ldots (p_r - 1),$$

unde $n=\varepsilon p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, $\varepsilon=\pm 1$, $p_1, p_2, \dots, p_r$ sînt numere prime pozitive diferite două cîte două, iar $\alpha_1, \alpha_2, \dots, \alpha_r$ sînt numere naturale.

Trecerea se face în felul următor. Avem, mai întîi,

$$\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right)=\sum_{s=0}^{r}\sum_{1\leqslant i_1<i_2<\dots<i_s\leqslant r}\frac{(-1)^s}{p_{i_1}p_{i_2}\dots p_{i_s}}=\sum_{d\mid p_1\dots p_r}\frac{\mu(d)}{d}=\sum_{d\mid n}\frac{\mu(d)}{d},$$

unde prin $\sum_{1\leqslant i_1<i_2<\dots<i_s\leqslant r}$ se înțelege că suma este extinsă la toate combinările $i_1\ i_2\ \dots\ i_s$ de r elemente $1, 2, \dots, r$ luate cîte s. Am notat $d=p_{i_1}p_{i_2}\dots p_{i_s}$ deci $d\mid p_1\dots p_r$ și $\mu(d)=(-1)^s$. Apoi am ținut seama că pentru oricare alt divizor d al lui n, deci diferit de divizorii lui $p_1\dots p_r$, avem $\mu(d)=0$ existînd cel puțin un factor prim p dintre $p_1, \dots, p_r$ astfel încît $p^2\mid d$. Transformările se fac mai departe în felul următor:

$$\varphi(n)=|n|\sum_{d\mid n}\frac{\mu(d)}{d}=|n|\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right)=p_1^{\alpha_1}\ p_2^{\alpha_2}\ \dots\ p_r^{\alpha_r}\cdot$$

$$\cdot\left(1-\frac{1}{p_1}\right)\cdot\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_r}\right)=p_1^{\alpha_1-1}p_2^{\alpha_2-1}\dots$$

$$\dots\ p_r^{\alpha_r-1}(p_1-1)(p_2-1)\dots(p_r-1).$$

Observație. Formula de calcul a valorilor funcției lui Euler

$$\varphi(n)=|n|\sum_{d\mid n}\frac{\mu(d)}{d}$$

poate fi stabilită și pe următoarea cale.

Vom arăta, mai întîi, că are loc următoarea:

Teoremă. *Avem*

$$\sum_{d\mid n}g(d)\sum_{1\leqslant k\leqslant\frac{x}{d}}h(kd)=\sum_{1\leqslant c\leqslant x}h(c)\sum_{d\mid(c,n)}g(d)$$

unde prin notația $\sum_{1\leqslant k\leqslant x}$ *se înțelege* $\sum_{k=1}^{[x]}$, $[x]$ *fiind partea întreagă a unui număr real* x, (c, n) *fiind cel mai mare divizor comun al numerelor întregi* c *și* n.

Demonstrație. Fie $M=\left\{(d, kd)\mid 1\leqslant k\leqslant\frac{x}{d}\ \&\ d\mid n\ \&\ d>0\right\}$, $N=\{(d, c)\mid 1\leqslant c\leqslant x\ \&\ d\mid(c, n)\ \&\ d>0\}$. Vom arăta că $M=N$. Într-adevăr, fie $(d, kd)\in M$. Atunci punînd $c=kd$ obținem $d\mid c$ și deoarece $d\mid n$ obținem $d\mid(c, n)$, (c, n) fiind cel mai mare divizor comun al lui c și n. Din $1\leqslant k\leqslant\frac{x}{d}$ și $d>0$ rezultă $1\leqslant d\leqslant kd\leqslant x$ sau $1\leqslant c\leqslant x$. Așadar $(d, kd)\in N$ și deci $M\subseteq N$. Fie acum $(d, c)\in N$. Din $d\mid(c, n)$, (c, n) fiind cel mai mare divizor comun al lui c și n, rezultă $d\mid c$, $d\mid n$. Deci există un număr natural k astfel încît $c=dk$. Atunci, din $1\leqslant c\leqslant x$ rezultă $1\leqslant kd\leqslant x$ și cum $d>0$ și $k>0$ din $kd\leqslant x$ rezultă $1\leqslant k\leqslant\frac{x}{d}$. Deci $(d, c)\in M$ și avem $N\subseteq M$. Rezultă că $M=N$.

În $\sum_{d\mid n}g(d)\sum_{1\leqslant k\leqslant\frac{x}{d}}h(kd)$ fiecare pereche (d, kd) din M apare o singură dată, iar în $\sum_{1\leqslant c\leqslant x}h(c)\sum_{d\mid(c,n)}g(d)$ fiecare pereche (d, c) din N apare o singură dată. Mulțimile M și N fiind egale, se constată că cele două sume sînt egale.

Putem da, acum, demonstrația următoarei teoreme:

Teoremă. *Dacă* $n\neq 0$ *atunci*

$$\varphi(n)=|n|\sum_{d\mid n}\frac{\mu(d)}{d}.$$

Demonstrație. Putem scrie

$$|n|\sum_{d\mid n}\frac{\mu(d)}{d}=\sum_{d\mid n}\mu(d)\frac{|n|}{d}.$$

Se constată că $\frac{|n|}{d}$ reprezintă numărul numerelor care se află în sistemul complet de resturi $1, 2, \dots, |n|$ modulo n și care se divid cu un divizor pozitiv d al lui n, deoarece aceste numere sînt

$$1\cdot d,\ 2\cdot d,\ \dots,\ \frac{|n|}{d}\,d.$$

Fie α o funcție definită pe mulțimea numerelor întregi astfel încît $\alpha(u)=1$ oricare ar fi numărul întreg u. Atunci

$$\frac{|n|}{d}=\alpha(1\cdot d)+\alpha(2\cdot d)+\dots+\alpha\left(\frac{|n|}{d}\,d\right)=\sum_{1\leqslant k\leqslant\frac{|n|}{d}}\alpha(kd).$$

Deci

$$|n| \sum_{d|n} \frac{\mu(d)}{d} = \sum_{d|n} \mu(d) \sum_{1 \leqslant k \leqslant \frac{|n|}{d}} \alpha(kd) = \sum_{1 \leqslant c \leqslant |n|} \alpha(c) \sum_{d|(c,n)} \mu(d)$$

(c, n) fiind cel mai mare divizor comun al numerelor întregi c și n. Dacă $(c, n) \neq 1$ avem $\sum_{d|(c,n)} \mu(d) = 0$, iar dacă $(c, n) \cong 1$ avem $\sum_{d|(c,n)} (\mu d) = 1$

Deci

$$\sum_{1 \leqslant c \leqslant |n|} \alpha(c) \sum_{d|(c,n)} \mu(d) = \sum_{\substack{1 \leqslant c \leqslant |n| \\ (c,n) \cong 1}} \alpha(c) = \varphi(n)$$

și am demonstrat această teoremă.

8.3. Formula de inversare a lui Moebius pentru funcțiile reale sau complexe de variabilă reală

Înainte de a da această formulă, vom da un mod de schimbare a ordinii de sumare pentru sumele de tipul $\sum_{1 \leqslant n \leqslant x} h(n)$, unde suma este extinsă la mulțimea numerelor naturale cel mult egale cu un număr real x, fiecare număr natural din această mulțime fiind luat o singură dată.

Teoremă. *Avem*

$$\sum_{1 \leqslant n \leqslant x} \left(\sum_{1 \leqslant m \leqslant \frac{x}{n}} h(m, mn) \right) = \sum_{1 \leqslant c \leqslant x} \left(\sum_{m|c} h(m, c) \right).$$

Demonstrație. Notăm cu M mulțimea tuturor perechilor (m, mn) astfel încît $1 \leqslant n \leqslant x$, $1 \leqslant m \leqslant \frac{x}{n}$, $M = \{(m, mn) \mid 1 \leqslant n \leqslant x \,\&\, 1 \leqslant m \leqslant \frac{x}{n}\}$, și cu N mulțimea tuturor perechilor (m, c) astfel încît $1 \leqslant c \leqslant x$, $m|c$, $m > 0$, $N = \{(m, c) \mid 1 \leqslant c \leqslant x \,\&\, m|c \,\&\, m > 0\}$. Vom arăta că $M = N$.

Într-adevăr, fie $(m, mn) \in M$. Atunci $1 \leqslant n \leqslant x$, $1 \leqslant m \leqslant \frac{x}{n}$. Din $1 \leqslant m \leqslant \frac{x}{n}$ deducem $n \leqslant mn \leqslant x$, deoarece $1 \leqslant n$, deci $n > 0$. Așadar

$1 \leqslant n \leqslant mn \leqslant x$, deci $1 \leqslant mn \leqslant x$. Notînd $c = mn$, obținem $1 \leqslant c \leqslant x$, $m|c$, $m > 0$, avînd $1 \leqslant m$, deci $(m, mn) \in N$, deci $M \subseteq N$. Fie acum $(m, c) \in N$. Atunci $1 \leqslant c \leqslant x$, $m|c$, $m > 0$. Din $m|c$ rezultă că există un număr întreg n astfel încît $c = mn$. Avem $n > 0$, deoarece $c > 0$ din $1 \leqslant c$ și $m > 0$. Din $1 \leqslant c \leqslant x$ și $c = mn$, $n > 0$ rezultă $1 \leqslant mn \leqslant x$ sau $1 \leqslant m \leqslant \frac{x}{n}$, deoarece din $m > 0$ rezultă $m \geqslant 1$. Apoi din $1 \leqslant mn \leqslant x$ rezultă $1 \leqslant n \leqslant x$, deoarece $n \leqslant mn$, ceea ce rezultă din $1 \leqslant m$ și $n > 0$, din ultima relație rezultînd și $1 \leqslant n$. Deci $N \subseteq M$ și am dovedit că $M = N$.

Perechile (m, mn) după care se face suma $\sum_{1 \leqslant n \leqslant x} \left(\sum_{1 \leqslant m \leqslant \frac{x}{n}} h(m, mn) \right)$ formează mulțimea M și fiecare din ele apare o singură dată în suma considerată, conform cu modul în care este definită această sumă. Perechile (m, c) după care se face suma $\sum_{1 \leqslant c \leqslant x} \left(\sum_{m|c} h(m, c) \right)$ formează mulțimea N și fiecare din ele apare o singură dată în suma considerată, conform cu modul în care este definită această sumă. Mulțimile M și N fiind egale, sînt egale și cele două sume considerate.

Formula de inversare a lui Moebius pentru funcțiile reale sau complexe de variabilă reală este conținută în următoarea teoremă.

Teoremă. *Dacă $P(n)$ este o funcție numerică total-multiplicativă, astfel încît $P(1) = 1$, iar $f(x)$ este o funcție numerică definită pentru orice număr real x pentru care $x \geqslant 1$, atunci din*

$$g(x) = \sum_{1 \leqslant n \leqslant x} P(n) f\left(\frac{x}{n}\right)$$

rezultă

$$f(x) = \sum_{1 \leqslant n \leqslant x} \mu(n) P(n) g\left(\frac{x}{n}\right)$$

și reciproc.

Demonstrație. Dacă

$$g(x) = \sum_{1 \leqslant n \leqslant x} P(n) f\left(\frac{x}{n}\right)$$

atunci

$$\sum_{1\leqslant n\leqslant x}\mu(n)\,P(n)\,g\left(\frac{x}{n}\right)=\sum_{1\leqslant n\leqslant x}\mu(n)\,P(n)\left(\sum_{1\leqslant m\leqslant\frac{x}{n}}P(m)f\left(\frac{\frac{x}{n}}{m}\right)\right)=$$

$$=\sum_{1\leqslant n\leqslant x}\sum_{1\leqslant m\leqslant\frac{x}{n}}\mu(n)P(n)P(m)f\left(\frac{x}{mn}\right)=\sum_{1\leqslant n\leqslant x}\sum_{1\leqslant m\leqslant\frac{x}{n}}\mu\left(\frac{mn}{m}\right)P(mn)f\left(\frac{x}{mn}\right)=$$

$$=\sum_{1\leqslant c\leqslant x}\sum_{m|c}\mu\left(\frac{c}{m}\right)P(c)\,f\left(\frac{x}{c}\right)=\sum_{1\leqslant c\leqslant x}P(c)\,f\left(\frac{x}{c}\right)\left(\sum_{m|c}\mu\left(\frac{c}{m}\right)\right)=$$

$$=P(1)\,f\left(\frac{x}{1}\right)=f(x),$$

deoarece atîta timp cît $c\neq 1$ avem $\sum_{m|c}\mu\left(\frac{c}{m}\right)=\sum_{m|c}\mu(m)=0$ și numai pentru $c=1$ avem $\sum_{m|1}\mu\left(\frac{1}{m}\right)=\sum_{m|1}\mu(m)=1$.

Reciproc, dacă

$$f(x)=\sum_{1\leqslant n\leqslant x}\mu(n)\,P(n)\,g\left(\frac{x}{n}\right)$$

atunci

$$\sum_{1\leqslant n\leqslant x}P(n)\,f\left(\frac{x}{n}\right)=\sum_{1\leqslant n\leqslant x}P(n)\left(\sum_{1\leqslant m\leqslant\frac{x}{n}}\mu(m)\,P(m)\,g\left(\frac{\frac{x}{n}}{m}\right)\right)=$$

$$=\sum_{1\leqslant n\leqslant x}\sum_{1\leqslant m\leqslant\frac{x}{n}}\mu(m)P(n)P(m)g\left(\frac{x}{mn}\right)=\sum_{1\leqslant n\leqslant x}\sum_{1\leqslant m\leqslant\frac{x}{n}}\mu(m)P(mn)g\left(\frac{x}{mn}\right)=$$

$$=\sum_{1\leqslant c\leqslant x}\sum_{m|c}\mu(m)\,P(c)\,g\left(\frac{x}{c}\right)=\sum_{1\leqslant c\leqslant x}P(c)\,g\left(\frac{x}{c}\right)\left(\sum_{m|c}\mu(m)\right)=$$

$$=P(1)\,g\left(\frac{x}{1}\right)=g(x),$$

deoarece atîta timp cît $c\neq 1$ avem $\sum_{m|c}\mu(m)=0$ și numai pentru $c=1$ avem $\sum_{m|c}\mu(m)=1$.

Să mai demonstrăm și următoarea teoremă.

Teoremă. *Avem*

$$\sum_{1\leqslant n\leqslant x}\left(\sum_{1\leqslant m\leqslant\frac{x}{n}}h(m,\,n)\right)=\sum_{1\leqslant m\leqslant x}\left(\sum_{1\leqslant n\leqslant\frac{x}{m}}h(m,\,n)\right).$$

Demonstrație. Notăm cu M mulțimea tuturor perechilor $(m,\,n)$ astfel încît $1\leqslant n\leqslant x$, $1\leqslant m\leqslant\frac{x}{n}$, $M=\left\{(m,n)\mid 1\leqslant n\leqslant x\,\&\,1\leqslant m\leqslant\frac{x}{n}\right\}$, și cu N mulțimea tuturor perechilor $(m,\,n)$ astfel încît $1\leqslant m\leqslant x$, $1\leqslant n\leqslant\frac{x}{m}$, $N=\left\{(m,n)\mid 1\leqslant m\leqslant x\,\&\,1\leqslant n\leqslant\frac{x}{m}\right\}$. Vom arăta că $M=N$.

Într-adevăr, fie $(m,\,n)\in M$. Atunci $1\leqslant n\leqslant x$, $1\leqslant m\leqslant\frac{x}{n}$, deci $n\leqslant mn\leqslant x$, deci $1\leqslant n\leqslant\frac{x}{m}$, deoarece $1\leqslant n$. Apoi $1\leqslant n$, deci $\frac{1}{n}\leqslant 1$, deci $\frac{x}{n}\leqslant x$, deoarece din $1\leqslant n\leqslant x$ rezultă $1\leqslant x$, deci $x>0$.

Cum $1\leqslant m\leqslant\frac{x}{n}$ rezultă $1\leqslant m\leqslant x$. Deci $(m,\,n)\in M$. Așadar $M\subseteq N$.

Demonstrația faptului că $N\subseteq M$ se obține schimbînd în demonstrația precedentă pe m cu n și pe n cu m. Deci $M=N$.

Perechile $(m,\,n)$ după care se formează suma $\sum_{1\leqslant n\leqslant x}\left(\sum_{1\leqslant m\leqslant\frac{x}{n}}h(m,\,n)\right)$ formează mulțimea M și fiecare din ele apare o singură dată în suma considerată, conform cu modul în care este definită această sumă. Perechile $(m,\,n)$ după care se formează suma $\sum_{1\leqslant m\leqslant x}\left(\sum_{1\leqslant n\leqslant\frac{x}{m}}h(m,\,n)\right)$ formează mulțimea N și fiecare din ele apare o singură dată în suma considerată, conform cu modul în care este definită această sumă. Deoarece mulțimile M și N sînt egale, sînt egale și cele două sume considerate.

Consecință.

$$\sum_{1\leqslant m\leqslant x}\left(\sum_{1\leqslant n\leqslant\frac{x}{m}}h(m,\,mn)\right)=\sum_{1\leqslant c\leqslant x}\left(\sum_{m|c}h(m,\,c)\right).$$

8.4. Funcția lui Mangoldt

Definiție. *Funcția lui Mangoldt notată cu* Λ *este o funcție numerică care are următoarele valori*

$$\Lambda(n)=\begin{cases}\log p & \text{dacă } n=\pm p^m,\\ 0 & \text{dacă } n\neq\pm p^m,\end{cases}$$

p fiind un număr natural prim, iar m fiind un număr natural.

Exemplu. $\Lambda(0)=0$, $\Lambda(\pm 1)=0$, $\Lambda(\pm 2)=2$, $\Lambda(\pm 3^3)=\log 3$.

Proprietăți ale funcției lui Mangoldt.

(1) *Dacă n este un număr întreg diferit de zero, atunci*

$$\sum_{d|n}\Lambda(d)=\log |n|,$$

suma fiind extinsă la mulțimea divizorilor pozitivi ai lui n, fiecare divizor fiind luat o singură dată.

Cu alte cuvinte, funcția de sumare a funcției lui Mangoldt este logaritmul.

Demonstrație. Avem

$$\sum_{d|n}\Lambda(d)=\sum_{p^\alpha|n}\log p,$$

suma din dreapta egalității fiind extinsă la toți divizorii pozitivi ai lui n care sînt puteri de numere prime cu exponentul număr natural, deoarece pentru divizorii d ai lui n diferiți de puteri de numere prime cu exponentul număr natural avem $\Lambda(d)=0$. Suma din dreapta egalității este deci egală cu zero pentru $n=\pm 1$. Dar în acest caz $\log |n|=0$ și deci proprietatea este demonstrată pentru $n=\pm 1$. Dacă $n\neq\pm 1$, atunci $|n|=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_r^{\alpha_r}$, în care, pentru p_i $(i=1, 2, \ldots, r)$ avem $\alpha_i\neq 0$ și deci p este egal fie cu p_1, fie cu p_2, ..., fie cu p_r, iar pentru p_i $(i=1, 2, \ldots, r)$ avem $\alpha=1, \ldots, \alpha_i$, deci

$$\sum_{p^\alpha|n}\log p=\sum_{\alpha=1}^{\alpha_1}\log p_1+\ldots+\sum_{\alpha=1}^{\alpha_2}\log p_r=$$

$$=\alpha_1\log p_1+\ldots+\alpha_r\log p_r=\log p_1^{\alpha_1}+\ldots+\log p_r^{\alpha_r}=$$

$$=\log p_1^{\alpha_1}\ldots p_r^{\alpha_r}=\log |n|.$$

(2) *Pentru* $n\neq 0$ *avem*

$$\Lambda(n)=\sum_{d|n}\mu(d)\log\frac{|n|}{d},$$

unde μ *este funcția lui Moebius.*

Demonstrație. Aplicînd formula de inversare a lui Moebius relației

$$\sum_{d|n}\Lambda(d)=\log |n|,$$

obținem

$$\Lambda(n)=\sum_{d|n}\mu(d)\log\frac{|n|}{d}.$$

8.5. Funcția $\Psi(x)$

Definiție. *Funcția* $\Psi(x)$ *este definită prin*

$$\Psi(x)=\sum_{1\leqslant n\leqslant x}\Lambda(n)$$

suma fiind extinsă la toate numerele naturale, diferite două cîte două, cel mult egale cu un număr real x.

Proprietăți ale funcției $\Psi(x)$.

1) $\Psi(x)=\log([1, 2, \ldots, [x]])$, *unde* $[1, 2, \ldots, [x]]$ *este cel mai mic multiplu comun al numerelor* $1, 2, \ldots, [x]$, $[x]$ *fiind partea întreagă a lui x.*

Într-adevăr, să notăm cu $p_1, \ldots, p_r$ toate numerele prime pozitive, diferite două cîte două, și cel mult egale cu x. Să notăm cu $p_1^{\alpha_1}, \ldots, p_r^{\alpha_r}$ puterile lor cele mai mari care sînt cel mult egale cu x, adică $\alpha_1, \ldots, \alpha_r$ sînt numere naturale alese astfel încît

$$p_1^{\alpha_1}\leqslant x<p_1^{\alpha_1+1}, \ldots, p_r^{\alpha_r}\leqslant x<p_r^{\alpha_r+1}$$

ceea ce se poate face luînd

$$\alpha_1=\left[\frac{\log x}{\log p_1}\right], \ldots, \alpha_r=\left[\frac{\log x}{\log p_r}\right].$$

Rezultă că

$$[1,\ 2,\ \ldots,\ [x]]=p_1^{\alpha_1}\,p_2^{\alpha_2}\ \ldots\ p_r^{\alpha_r},$$

deoarece divizorii primi pozitivi ai numerelor 1, 2, ..., $[x]$ nu pot fi decît p_1, ..., p_r orice număr prim pozitiv diferit de p_1, ..., p_r fiind mai mare ca x și deci neputînd divide pe nici unul dintre 1, 2, ..., $[x]$ care sînt cel mult egale cu x și apoi oricare dintre 1, 2, ..., $[x]$ cuprinde pe p_i ca factor cel mult la puterea α_i, deoarece dacă am avea $p_i^{\beta}k\leqslant x$ cu $\beta>\alpha_i$ am avea și $p_i^{\alpha_i+1}\leqslant p_i^{\beta}\leqslant p_i^{\beta}k\leqslant x$, deci $p_i^{\alpha_i+1}\leqslant x$, ceea ce este absurd.

Deci

$$[1,\ 2,\ \ldots,\ [x]]=[1,\ \ldots,\ p_1^{\alpha_1},\ \ldots,\ p_r^{\alpha_r},\ \ldots,\ [x]]=p_1^{\alpha_1}\,p_2^{\alpha_2}\ldots p_r^{\alpha_r}$$

cel mai mic multiplu comun al mai multor numere fiind produsul factorilor primi comuni și necomuni la puterea cea mai mare, fiecare factor prim fiind luat o singură dată.

În ceea ce privește funcția $\Psi(x)$ avem

$$\Psi(x)=\sum_{1\leqslant n\leqslant x}\Lambda(n)=\sum_{p^m\leqslant x}\log\,p,$$

ultima sumă fiind extinsă numai la puteri de numere prime pozitive cel mult egale cu x, deoarece $\Lambda(n)=0$ pentru $n\neq\pm p^m$. Ținînd seama de faptul că p_1, ..., p_r sînt toate numerele prime pozitive diferite două cîte două și cel mult egale cu x și ținînd seama și de faptul că $p_1^{\alpha_1}\leqslant x<p_1^{\alpha_1+1}$, ..., $p_r^{\alpha_r}\leqslant x<p_r^{\alpha_r+1}$, rezultă că

$$\Psi(x)=\sum_{\beta_1=1}^{\alpha_1}\log\,p_1+\ldots+\sum_{\beta_r=1}^{\alpha_r}\log\,p_r=\sum_{i=1}^{r}\alpha_i\log\,p_i=$$

$$=\log\,(p_1^{\alpha_1}\ \ldots\ p_r^{\alpha_r})=\log\,([1,\ 2,\ \ldots,\ [x]]).$$

(2) $\Psi(x)=\sum_{p\leqslant x}\left[\frac{\log\,x}{\log\,p}\right]\log\,p$, *suma fiind extinsă la toate numerele prime pozitive, diferite două cîte două, cel mult egale cu un număr real* x.

Într-adevăr, din demonstrația proprietății precedente rezultă

$$\Psi(x)=\sum_{i=1}^{r}\alpha_i\log\,p_i=\sum_{i=1}^{r}\left[\frac{\log\,x}{\log\,p_i}\right]\log\,p_i=\sum_{p\leqslant x}\left[\frac{\log\,x}{\log\,p}\right]\log\,p,$$

p_1, ..., p_r fiind toate numerele prime pozitive diferite două cîte două și cel mult egale cu x.

Capitolul 9

NUMĂRUL NUMERELOR PRIME

9.1. Funcția $\varphi(x,\ r)$

Definiție. *Numărul numerelor naturale cel mult egale cu un număr real* x *și care nu se divid cu nici unul din primele* r *numere prime pozitive este o funcție numerică care se notează cu* $\varphi(x,\ r)$.

Proprietăți ale funcției $\varphi(x,\ r)$.

(1) $\varphi(x,\ r)=\varphi(x,\ r-1)-\varphi(xp_r^{-1},\ r-1)$, *unde* p_r *este al* r*-lea număr prim pozitiv.*

Demonstrație. Să considerăm numerele naturale cel mult egale cu un număr real x și care nu se divid cu nici unul din primele $r-1$ numere prime pozitive. Numărul lor este $\varphi(x,\ r-1)$. Printre aceste numere se află atît numere care nu se divid cu p_r, cît și numere care se divid cu p_r, unde p_r este al r-lea număr prim pozitiv. Cele care nu se divid cu p_r au deci proprietatea că sînt cei mult egale cu x și nu se divid cu nici unul din primele r numere prime pozitive. Numărul lor este deci egal cu $\varphi(x,\ r)$. Cele care se divid cu p_r sînt de forma hp_r, unde h este orice număr natural cu proprietatea că $h\leqslant xp_r^{-1}$, deoarece $hp_r\leqslant x$. Numerele considerate, anume hp_r, nu se divid cu primele $r-1$ numere prime pozi-

tive, deci h nu se divide cu primele $r-1$ numere prime pozitive. Numărul numerelor h este deci egal cu $\varphi(xp_r^{-1}, r-1)$. Avem deci

$$\varphi(x, r-1)=\varphi(x, r)+\varphi(xp_r^{-1}, r-1),$$

de unde rezultă relația din enunț.

(2) *Dacă* $[x]=qp_1p_2\ldots p_r+k$, *în care* q *și* k *sînt numere întregi nenegative, iar* $p_1, p_2, \ldots, p_r$ *sînt primele* r *numere prime pozitive, atunci* $\varphi(x, r)=q\varphi(p_1p_2\ldots p_r)+\varphi(k, r)$, $\varphi(p_1p_2\ldots p_r)$ *fiind indicatorul lui Euler al lui* $p_1p_2\ldots p_r$.

Demonstrație. Dacă $q>0$, atunci de la 1 la $p_1p_2\ldots p_r$, apoi de la $p_1p_2\ldots p_r+1$ la $2p_1p_2\ldots p_r$ ș.a.m.d. pînă la $qp_1p_2\ldots p_r$ avem q sisteme complete de resturi modulo $p_1p_2\ldots p_r$. În fiecare din aceste sisteme complete de resturi, numerele care nu se divid cu p_1, $p_2, \ldots, p_r$ sînt prime cu modulul $p_1p_2\ldots p_r$ și reciproc, deci sînt în număr de $\varphi(p_1p_2\ldots p_r)$ și în total sînt în număr de $q\,\varphi(p_1p_2\ldots p_r)$.

Mai trebuie determinat numărul numerelor naturale care nu se divid cu $p_1, p_2, \ldots, p_r$ și care sînt mai mari decît $qp_1p_2\ldots p_r$ și cel mult egale cu $qp_1p_2\ldots p_r+k$, deoarece între $[x]=qp_1p_2\ldots p_r+k$ și x nu se mai află nici un număr întreg. Aceste numere sînt de forma $qp_1p_2\ldots p_r+i$ cu $1\leqslant i\leqslant k$. Dacă $qp_1p_2\ldots p_r+i$ nu se divide cu p_j, $1\leqslant j\leqslant r$, atunci nici i nu se divide cu p_j și reciproc. Deci numărul numerelor de forma $qp_1p_2\ldots p_r+i$ cu $1\leqslant i\leqslant k$ care nu se divid cu $p_1, p_2, \ldots, p_r$ este egal cu numărul numerelor i cu $1\leqslant i\leqslant k$ care nu se divid cu $p_1, p_2, \ldots, p_r$. Numărul acestor ultime numere este egal cu $\varphi(k, r)$. Deci am demonstrat relația

$$\varphi(x, r)=q\varphi(p_1p_2\ldots p_r)+\varphi(k, r),$$

atît pentru $q>0$ cît și pentru $q=0$, deoarece pentru $q=0$ avem $q\varphi(p_1p_2\ldots p_r)=0$, iar numerele naturale cel mult egale cu x și care nu se divid cu $p_1, p_2, \ldots, p_r$ sînt toate de forma $qp_1p_2\ldots p_r+i$ cu $1\leqslant i\leqslant k$, deoarece sînt de fapt de forma i cu $1\leqslant i\leqslant k$ avînd în vedere că $q=0$.

(3) $\varphi(p_1p_2\ldots p_r, r)=\varphi(p_1p_2\ldots p_r)$.

Demonstrație. $\varphi(p_1p_2\ldots p_r, r)$ este numărul numerelor naturale nedivizibile cu $p_1, p_2, \ldots, p_r$ deci prime cu $p_1p_2\ldots p_r$ și cel mult egale cu $p_1p_2\ldots p_r$, ceea ce este același lucru cu $\varphi(p_1p_2\ldots p_r)$.

(4) $\varphi(p_1p_2\ldots p_r, r)=2\varphi(p_2\ldots p_r, r)$.

Demonstrație. Avem $p_1p_2\ldots p_r=2p_2\ldots p_r$, deoarece $p_1=2$. Deci numerele naturale cel mult egale cu $p_1p_2\ldots p_r$ pot fi împărțite în două intervale : unul de la 1 la $p_2\ldots p_r$, al doilea de la $p_2\ldots p_r+1$ la $p_2\ldots p_r+p_2\ldots p_r$. Fiecărui număr $i\neq p_2\ldots p_r$ din primul interval îi corespunde un singur număr $p_1p_2\ldots p_r-i$ din al doilea interval, lui $p_2\ldots p_r$ din primul interval făcîndu-i să corespundă $p_2\ldots p_r+p_2\ldots p_r=p_1p_2\ldots p_r$. Dacă i nu se divide cu nici unul din $p_1, p_2, \ldots, p_r$, atunci nici numărul $p_1p_2\ldots p_r-i$ nu se divide cu nici unul din $p_1, p_2, \ldots, p_r$ și reciproc. Deci numerele naturale care nu se divid cu nici unul din $p_1, p_2, \ldots, p_r$ se găsesc în mod egal în cele două intervale, iar în primul interval se află de un număr de ori egal cu $\varphi(p_2\ldots p_r, r)$.

Observație. Proprietatea (3) ne arată că funcția $\varphi(x, r)$ generalizează funcția lui Euler. Proprietățile (1) și (2) ale funcției $\varphi(x, r)$ permit și calculul acestei funcții.

(5) *Dacă* $x\geqslant 0$, *atunci* $\varphi(x, r)=\sum_{d\mid p_1p_2\ldots p_r}\mu(d)\left[\frac{x}{d}\right]$, *unde* μ *este funcția lui Moebius.*

Prima demonstrație. Vom face raționamentul prin inducție completă după valorile lui r, începînd cu $r=0$.

Avem $\varphi(x, 0)=[x]$, fiindcă toate numerele naturale cel mult egale cu x, al căror număr este $[x]$, nu se divid cu nici unul din primele 0 numere prime pozitive, acestea neexistînd. Apoi

$$\sum_{d\mid p_1p_2\ldots p_0}\mu(d)\left[\frac{x}{d}\right]=\sum_{d\mid 1}\mu(d)\left[\frac{x}{d}\right]=[x]$$

și avem $\varphi(x, 0)=\sum_{d\mid p_1p_2\ldots p_0}\mu(d)\left[\frac{x}{d}\right]$, deoarece se consideră că atunci cînd în produsul $p_1p_2\ldots p_r$ nu există nici un factor, caz care are loc pentru $r=0$, atunci produsul considerat este egal cu 1.

Presupunem acum că

$$\varphi(y, r-1)=\sum_{d\mid p_1p_2\ldots p_{r-1}}\mu(d)\left[\frac{y}{d}\right]$$

oricare ar fi numărul real $y \geqslant 0$. După proprietatea (1) avem

$$\varphi(x,\ r)=\varphi(x,\ r-1)-\varphi(xp_r^{-1},r-1)=\sum_{d|p_1p_2\ldots p_{r-1}}\mu(d)\left[\frac{x}{d}\right]-$$

$$-\sum_{d|p_1p_2\ldots p_{r-1}}\mu(d)\left[\frac{xp_r^{-1}}{d}\right].$$

Ultima sumă se mai scrie

$$\sum_{d|p_1p_2\ldots p_{r-1}}\mu(d)\left[\frac{x}{dp_r}\right]=-\sum_{d|p_1p_2\ldots p_{r-1}}\mu(d)\mu(p_r)\left[\frac{x}{dp_r}\right]=$$

$$=-\sum_{dp_r|p_1p_2\ldots p_r}\mu(dp_r)\left[\frac{x}{dp_r}\right].$$

Divizorii lui $p_1p_2\ldots p_r$ pot fi împărțiți în două categorii: unii care se compun numai din $p_1,\ p_2,\ \ldots,\ p_{r-1}$, deci sînt divizorii lui $p_1p_2\ldots p_{r-1}$, alții care conțin și pe p_r deci sînt de forma dp_r unde $d|p_1p_2\ldots p_{r-1}$. Din această cauză și ținînd seama de sumele de mai sus, avem

$$\varphi(x,\ r)=\sum_{d|p_1p_2\ldots p_r}\mu(d)\left[\frac{x}{d}\right]$$

și proprietatea (5) este demonstrată.

A doua demonstrație. Ținem seama de faptul că numărul numerelor naturale cel mult egale cu x și care se divid cu numărul natural d este egal cu $\left[\frac{x}{d}\right]$ în cazul cînd $x \geqslant 0$. Într-adevăr, dacă notăm cu td cel mai mare număr natural cel mult egal cu x care se divide cu d, avem

$$td \leqslant x < (t+1)d$$

deci

$$t \leqslant \frac{x}{d} < t+1,$$

de unde $t=\left[\frac{x}{d}\right]$. Numerele naturale care se divid cu d și sînt cel mult egale cu x sînt

$$1\cdot d,\ 2\cdot d,\ \ldots,\ t\cdot d,$$

deci numărul lor este $t=\left[\frac{x}{d}\right]$. Fie α o funcție definită pe mulțimea

numerelor întregi astfel încît $\alpha(u)=1$ oricare ar fi numărul întreg u. Atunci

$$\left[\frac{x}{d}\right]=\alpha(1\cdot d)+\alpha(2\cdot d)+\ldots+\alpha\left(\left[\frac{x}{d}\right]d\right)=\sum_{1\leqslant k\leqslant\frac{x}{d}}\alpha(kd),$$

deoarece între $\left[\frac{x}{d}\right]$ și $\frac{x}{d}$ nu se mai află nici un număr întreg. Deci

$$\sum_{d|p_1p_2\ldots pr}\mu(d)\left[\frac{x}{d}\right]=\sum_{d|p_1p_2\ldots pr}\mu(d)\sum_{1\leqslant k\leqslant\frac{x}{d}}\alpha(kd)=$$

$$=\sum_{1\leqslant c\leqslant x}\alpha(c)\sum_{d|(c,p_1p_2\ldots p_r)}\mu(d)$$

$(c,\ p_1p_2\ldots p_r)$ fiind cel mai mare divizor comun al numerelor întregi c și $p_1p_2\ldots p_r$. Dacă $(c,\ p_1p_2\ldots p_r)\cong 1$ avem $\sum_{d|(c,p_1p_2\ldots p_r)}\mu(d)=0$, iar dacă $(c,\ p_1p_2\ldots p_r)\cong 1$ avem $\sum_{d|(c,p_1p_2\ldots p_r)}\mu(d)=1$. Deci

$$\sum_{1\leqslant c\leqslant x}\alpha(c)\sum_{d|(c,p_1p_2\ldots p_r)}\mu(d)=\sum_{\substack{1\leqslant c\leqslant x\\(c,p_1p_2\ldots p_r)\cong 1}}\alpha(c)=\varphi(x,\ r)$$

și am demonstrat teorema, pentru că numerele naturale cel mult egale cu x și prime cu $p_1p_2\ldots p_r$ sînt și nedivizibile cu $p_1, p_2, \ldots, p_r$ și reciproc.

9.2. Funcția $\pi(x)$

Definiție. *Numărul numerelor prime pozitive cel mult egale cu un număr real x este o funcție numerică care se notează cu $\pi(x)$.*

Exemple. $\pi(1)=0,\ \pi(2)=1,\ \pi(\sqrt{5})=1,\ \pi(20)=8.$

Proprietăți ale funcției $\pi(x)$.

(1) *Dacă* $1 \leqslant a \leqslant b \leqslant a^2$, *atunci* $\varphi(b,\ \pi(a))=1+\pi(b)-\pi(a)$.

Demonstrație. Numărul numerelor naturale cel mult egale cu b și care nu se divid cu nici unul dintre primele $\pi(a)$ numere prime pozitive este egal cu $\varphi(b,\ \pi(a))$. Numerele naturale n cel mult

egale cu b pot fi împărțite în următoarele categorii $n=1$, $1<n\leqslant a$, $a<n\leqslant b$. Printre numerele naturale cel mult egale cu b și care nu se divid cu nici unul dintre primele $\pi(a)$ numere prime pozitive se află $n=1$, deoarece 1 nu se divide cu nici un număr prim. Printre numerele naturale cel mult egale cu b și care nu se divid cu nici unul dintre primele $\pi(a)$ numere prime pozitive nu se află nici un număr natural n pentru care $1<n\leqslant a$. Într-adevăr, există un număr prim p pozitiv astfel ca $p|n$, deci $n=pk$ cu $k\geqslant 1$ și deci din $n\leqslant a$ rezultă $a\geqslant pk\geqslant p$, deci p este printre primele $\pi(a)$ numere prime pozitive, aceste numere prime pozitive fiind cel mult egale cu a. Printre numerele naturale cel mult egale cu b și care nu se divid cu nici unul dintre primele $\pi(a)$ numere prime pozitive, se află numai numerele prime pozitive n pentru care $a<n\leqslant b$ și al căror număr este egal cu $\pi(b)-\pi(a)$. Într-adevăr, orice număr prim n pentru care $a<n\leqslant b$ nu se divide cu nici unul din primele $\pi(a)$ numere prime pozitive, pentru că acestea sînt cel mult egale cu a, pe cînd $a<n$. Dacă n este compus și $a<n\leqslant b$, notînd cu p cel mai mic număr prim pozitiv care-l divide pe n, putem scrie $n=pk$ cu $k\geqslant p$, numerele prime care divid pe k fiind cel puțin egale cu p, p fiind cel mai mic număr prim pozitiv care-l divide pe n, iar divizorii lui k fiind și divizori ai lui n. Din cauză că $b\leqslant a^2$, iar $n\leqslant b$ avem $a^2\geqslant pk\geqslant p^2$, deci $p\leqslant a$, deci p este printre primele $\pi(a)$ numere prime pozitive, aceste numere prime pozitive fiind cel mult egale cu a. Deci numerele naturale cel mult egale cu b și care nu se divid cu nici unul dintre primele $\pi(a)$ numere prime pozitive sînt numărul 1 și numerele prime pozitive n astfel încît $a<n\leqslant b$, deci proprietatea (1) este demonstrată.

(2) *Dacă* $x\geqslant 1$, *atunci* $\pi(x)=\pi(\sqrt{x})+\varphi(x,\ \pi(\sqrt{x}))-1$.

Demonstrație. În proprietatea (1) punem $a=\sqrt{x}$, $b=x$.

(3) *Dacă* $x\geqslant 4$, *iar* $m=\pi(x^{\frac{1}{3}})$, $n=\pi(x^{\frac{1}{2}})$, $s=n-m$, *atunci*

$$\pi(x)=\varphi(x,\ m)+m(s+1)+\frac{s(s-1)}{2}-1-\sum_{t=1}^{s}\pi\left(\frac{x}{p_{m+t}}\right).$$

Demonstrație. Din proprietatea (2) deducem

$$\pi(x)=n+\varphi(x,\ n)-1.$$

Avem

$$\varphi(x,\ n)=\varphi(x,\ n-1)-\varphi(xp_n^{-1},\ n-1),$$
$$\varphi(x,\ n-1)=\varphi(x,\ n-2)-\varphi(xp_{n-1}^{-1},\ n-2),$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\varphi(x,\ m+1)=\varphi(x,\ m)-\varphi(xp_{m+1}^{-1},\ m),$$

deci

$$\varphi(x,\ n)=\varphi(x,\ m)-\sum_{t=1}^{s}\varphi(xp_{m+t}^{-1},\ m+t-1).$$

Din cauză că $\pi(x^{\frac{1}{3}})=m$, avem $x^{\frac{1}{3}}<p_{m+t}$ pentru orice $t\geqslant 1$. Din cauză că $\pi(x^{\frac{1}{2}})=n=m+s$ avem $p_{m+t}\leqslant x^{\frac{1}{2}}$ pentru orice t pentru care $1\leqslant t\leqslant s$. Deci.

$$x^{\frac{1}{3}}<p_{m+t}\leqslant x^{\frac{1}{2}}$$

pentru orice $t=1,\ 2,\ \ldots,\ s$. Din $x^{\frac{1}{3}}<p_{m+t}$ rezultă $x^{\frac{2}{3}}x^{\frac{1}{3}}p_{m+t}^{-1}<x^{\frac{2}{3}}$ deci $xp_{m+t}^{-1}<x^{\frac{2}{3}}$. Din $p_{m+t}\leqslant x^{\frac{1}{2}}$ rezultă $x^{\frac{1}{2}}\leqslant x^{\frac{1}{2}}x^{\frac{1}{2}}p_{m+t}^{-1}$, deci $x^{\frac{1}{2}}\leqslant xp_{m+t}^{-1}$. Avem, prin urmare,

$$p_{m+t}\leqslant x^{\frac{1}{2}}\leqslant xp_{m+t}^{-1}<x^{\frac{2}{3}}<p_{m+t}^2$$

de unde reținem

$$p_{m+t}\leqslant xp_{m+t}^{-1}<p_{m+t}^2$$

și cum $1<p_{m+t}$, punînd în proprietatea (1) $a=p_{m+t}$, $b=xp_{m+t}^{-1}$, deducem

$$\varphi(xp_{m+t}^{-1},\ m+t)=1+\pi(xp_{m+t}^{-1})-(m+t),$$

deoarece din $a=p_{m+t}$ rezultă $\pi(a)=m+t$. Trebuie să avem $x\geqslant 4$, ca să nu contrazicem relația $p_{m+t}\leqslant x^{1/2}$, deoarece $2\leqslant p_{m+t}$.

Avem

$$\varphi(xp_{m+t}^{-1},m+t)=\varphi(xp_{m+t}^{-1},\ m+t-1)-\varphi(xp_{m+t}^{-2},\ m+t-1).$$

Din $p_{m+t} \leqslant x p_{m+t}^{-1} < p_{m+t}^2$ deducem $1 \leqslant x p_{m+t}^{-2} < p_{m+t}$, deci orice număr natural diferit de 1 cel mult egal cu $x p_{m+t}^{-2}$ fiind strict mai mic ca p_{m+t} este divizibil cu cel puțin unul din primele $m+t-1$ numere prime pozitive, deci

$$\overline{\varphi}(x p_{m+t}^{-2},\ m+t-1)=1,$$

avînd $1 \leqslant x p_{m+t}^{-2}$. Obținem

$$\varphi(x p_{m+t}^{-1}, m+t-1)=\varphi(x p_{m+t}^{-1},\ m+t)+\varphi(x p_{m+t}^{-2},\ m+t-1)=$$

$$=\pi(x p_{m+t}^{-1})-(m+t-2).$$

Așadar

$$\pi(x)=m+s+\varphi(x,m)-\sum_{t=1}^{s}\pi(x p_{m+t}^{-1})+\sum_{t=1}^{s}(m-2+t)-1=$$

$$=m+s+\varphi(x,m)-\sum_{t=1}^{s}\pi(x p_{m+t}^{-1})+(m-2)s+\frac{s(s+1)}{2}-1,$$

de unde rezultă formula din enunțul proprietății (3).

Observație. Această formulă permite calculul numărului numerelor prime pozitive cel mult egale cu un număr real $x \geqslant 4$, cunoscînd un număr redus de numere prime anume acele care satisfac relația $x^{1/3} < p \leqslant x^{1/2}$. Deoarece această formulă este o formulă de recurență, valorile lui $\pi(x)$ fiind deduse în funcție de valorile lui $\pi\left(\frac{x}{p}\right)$ cu $x^{1/3} < p \leqslant x^{1/2}$, înseamnă că este suficient să cunoaștem toate numerele prime pozitive cel mult egale cu $x^{1/2}$, iar nu cel mult egale cu x, cum am face dacă le-am număra.

Exemplu. Să-l calculăm pe $\pi(1\,000)$.

Avem $1\,000^{1/2}=31{,}6\ldots$ și $1\,000^{1/3}=10$. Trebuie să calculăm $\pi(31{,}6\ldots)=\pi(31{,}6)$ și $\pi(10)$. În acest scop ne trebuie $31{,}6^{1/2}=5, \ldots$, $31{,}6^{1/3}=3, \ldots$ deci $\pi(31{,}6^{1/2})=\pi(5, \ldots)=3$, $\pi(31{,}6^{1/3})=\pi(3, \ldots)=2$ și $\pi(10)=4$. Ultimele trei valori ale lui $\pi(x)$ le-am calculat prin numărare. Avem, cu formula dată de (3),

$$\pi(31{,}6)=\varphi(31{,}6,\ 2)+2(1+1)+\frac{1\cdot(1-1)}{2}-1-\sum_{t=1}^{1}\pi\left(\frac{31{,}6}{p_{2+t}}\right)=$$

$$=\varphi(31{,}6,\ 2)+3-\pi\left(\frac{31{,}6}{5}\right).$$

Din cauză că $[31{,}6]=31=5(2\cdot 3)+1$ avem $\varphi(31{,}6\ ,2)=5\varphi(2\cdot 3)+\varphi(1,\ 2)=5(2-1)(3-1)+1=11$. Deci

$$\pi(31{,}6)=11+3-\pi(6{,}3\ldots)=11,\quad s=\pi(31{,}6)-\pi(10)=11-4=7.$$

Deci

$$\pi(1\,000)=\varphi(1\,000,4)+4(7+1)+\frac{7(7-1)}{2}-1-\sum_{t=1}^{7}\pi\left(\frac{1\,000}{p_{4+t}}\right),$$

unde $p_5=11$, $p_6=13$, $p_7=17$, $p_8=19$, $p_9=23$, $p_{10}=29$, $p_{11}=31$. Prin numărarea numerelor prime pozitive obținem

$$\pi\left(\frac{1\,000}{11}\right)=\pi(90)=24,\quad \pi\left(\frac{1\,000}{13}\right)=\pi(76)=21,\quad \pi\left(\frac{1\,000}{17}\right)=$$

$$=\pi(58)=16,\quad \pi\left(\frac{1\,000}{19}\right)=\pi(52)=15,\quad \pi\left(\frac{1\,000}{23}\right)=\pi(43)=$$

$$=14,\quad \pi\left(\frac{1\,000}{29}\right)=\pi(34)=11,\quad \pi\left(\frac{1\,000}{31}\right)=\pi(32)=11.$$

Deci

$$\sum_{t=1}^{7}\pi\left(\frac{1\,000}{p_{4+t}}\right)=112.$$

Avem în vedere că

$$\varphi(1\,000,4)=\varphi(1\,000,3)-\varphi\left(\frac{1\,000}{7},3\right)=\varphi(1\,000,\ 2)-\varphi\left(\frac{1\,000}{5},\ 2\right)-$$

$$-\varphi(142,2)+\varphi\left(\frac{142}{5},\ 2\right)=\varphi(1\,000,1)-\varphi\left(\frac{1\,000}{3},\ 1\right)-$$

$$-\varphi(200,1)+\varphi\left(\frac{200}{3},\ 1\right)-\varphi(142,1)+\varphi\left(\frac{142}{3},\ 1\right)+$$

$$+\varphi(28,1)-\varphi\left(\frac{28}{3},\ 1\right)=\varphi(1\,000,0)-\varphi\left(\frac{1\,000}{2},\ 0\right)-$$

$$-\varphi(333,0)+\varphi\left(\frac{333}{2},\ 0\right)-\varphi(200,0)+\varphi\left(\frac{200}{2},\ 0\right)+$$

$$+\varphi(66,0)-\varphi\left(\frac{66}{2},\ 0\right)-\varphi(142,0)+\varphi\left(\frac{142}{2},\ 0\right)+$$

$$+\varphi(47,0)-\varphi\left(\frac{47}{2},\ 0\right)+\varphi(28,0)-\varphi\left(\frac{28}{2},\ 0\right)-\varphi(9,0)+$$

$$+\varphi\left(\frac{9}{2},\ 0\right)=1\,000-500-333+166-200+100+66-33-$$

$$-142+71+47-23+28-14-9+4=1\,482-1\,254=228.$$

Deci

$$\pi(1\,000)=228+32+21-1-112=168.$$

(4) *Pentru* $x\geqslant 2$ *avem* $\pi(x)>(2\log 2)^{-1}\log x$.

Demonstrație. Orice număr natural n poate fi scris ca un produs dintre un pătrat perfect și un număr natural care nu are nici un factor pătrat perfect. Acest lucru rezultă din reprezentarea numerelor naturale sub formă de produse de un număr finit de factori primi pozitivi, în felul următor :

$$n=p_1^{\alpha_1}\ldots p_r^{\alpha}r=p_{i_1}^{2\beta_1}\ldots\ p_{i_s}^{2\beta_s}\ p_{i_{s+1}}^{2\gamma_{s+1}+1}\ \ldots p_{i_r}^{2\gamma_r+1}=$$

$$=\left(p_{i_1}^{\beta_1}\ldots\ p_{i_s}^{\beta_s}p_{i_{s+1}}^{\gamma_{s+1}}\ldots\ p_{i_r}^{\gamma r}\right)^2 p_{i_{s+1}}\ldots\ p_{ir}=a^2b,$$

unde

$$a=p_{i_1}\ \ldots\ p_{i_s}p_{i_{s+1}}\ \ldots\ p_{ir},\quad b=p_{i_{s+1}}\ldots\ p_{ir},$$

deoarece o parte din exponenții $\alpha_1,\ \ldots,\ \alpha_r$ sînt pari și pe aceștia i-am notat cu $\alpha_{i_1}=2\beta_1,\ \ldots,\ \alpha_{i_s}=2\beta_s$, iar ceilalți dintre exponenții $\alpha_1,\ \ldots,\ \alpha_r$ sînt impari și pe aceștia i-am notat cu $\alpha_{i_{s+1}}=2\gamma_{s+1}+1,\ \ldots,\ \alpha_{i_r}=2\gamma_r+1$.

Dacă x este un număr real pozitiv și presupunem că

$$n\leqslant x$$

atunci obținem că

$$a^2\leqslant x,\quad b\leqslant x.$$

Notînd cu k partea întreagă a lui $\sqrt{x}$ obținem că $k\leqslant\sqrt{x}<k+1$, deci

$$k^2\leqslant x<(k+1)^2.$$

Acest număr natural k reprezintă și numărul pătratelor perfecte care sînt cel mult egale cu x, deoarece aceste pătrate perfecte sînt numai $1^2,\ 2^2,\ \ldots,\ k^2$, iar $1\leqslant k$, deoarece $1\leqslant\sqrt{x}$, avînd $x\geqslant 2$.

Din $b\leqslant x$ rezultă că numai numerele prime $p_1,\ \ldots,\ p_{\pi(x)}$ pozitive, care sînt cel mult egale cu x, pot să-l dividă pe b, deoarece dacă prin absurd un număr prim p mai mare ca x îl divide pe b,

atunci din $p\mid b$ și $b\leqslant x$ ar rezulta $p\leqslant x$, ceea ce este contradictoriu. Așadar, factorii primi pozitivi ai lui b pot fi numai numerele prime pozitive $p_1,\ \ldots,\ p_{\pi(x)}$, iar b fiind fără factori pătrate perfecte, rezultă că b este divizorul produsului $p_1\ldots p_{\pi(x)}$.

Deci orice număr natural cel mult egal cu x se obține înmulțind un pătrat perfect cel mult egal cu x, cu un divizor pozitiv al lui $p_1\ldots p_{\pi(x)}$. Deci

$$[x]\leqslant k2^{\pi(x)},$$

deoarece $[x]$ reprezintă numărul numerelor naturale cel mult egale cu x, iar $k2^{\pi(x)}$ reprezintă numărul produselor dintre pătratele perfecte cel mult egale cu x și divizorii pozitivi ai lui $p_1\ldots p_{\pi(x)}$, numărul acestor divizori pozitivi fiind egal cu $2^{\pi(x)}$.

Avem

$$[x]=k2^{\pi(x)}$$

numai dacă

$$[x]=k^2p_1\ldots p_{\pi(x)},$$

numărul natural $k^2p_1\ldots p_{\pi(x)}$ fiind cel mai mare dintre produsele dintre pătratele perfecte cel mult egale cu x și divizorii pozitiv ai lui $p_1\ldots p_{\pi(x)}$.

Din $[x]=k2^{\pi(x)}$ și $[x]=k^2p_1\ldots p_{\pi(x)}$ rezultă

$$k2^{\pi(x)}=k^2p_1\ldots p_{\pi(x)}$$

sau

$$2^{\pi(x)}=kp_1\ldots p_{\pi(x)}$$

k fiind un număr natural, deoarece am presupus că $x\geqslant 2$. Deci

$$2^{\pi(x)}\geqslant k2^{\pi(x)},$$

deoarece $p_1\ldots p_{\pi(x)}\geqslant 2^{\pi(x)}$. Rezultă $k=1$. Deci

$$2^{\pi(x)}=p_1\ldots p_{\pi(x)},$$

de unde rezultă că $\pi(x)=1$, deoarece dacă $\pi(x)>1$, avem $2^{\pi(x)}<p_1\ldots p_{\pi(x)}$. Din $\pi(x)=1$ rezultă că $2\leqslant x<3$. Presupunînd că $x\geqslant 3$ avem

$$[x]<k2^{\pi(x)}$$

deci $[x]+1\leqslant k2^{\pi(x)}$ deci $x<k2^{\pi(x)}$ sau $x<\sqrt{x}\ 2^{\pi(x)}$ sau $\sqrt{x}<2^{\pi(x)}$, ceea ce este adevărat și în cazul cînd $2\leqslant x<3$, deoarece avem $\sqrt{x}<2$ în acest caz, ceea ce concordă cu $\pi(x)=1$. Din $\sqrt{x}<2^{\pi(x)}$ prin logaritmare obținem $\frac{1}{2}\log x<\pi(x)\log 2$, deci

$$\pi(x)>(2\log 2)^{-1}\log x.$$

Capitolul 10

CARACTERE MODULO m

10.1. Definiția caracterelor modulo m

Caracter modulo m este o funcție numerică care se notează cu χ și are următoarele proprietăți :

(*A*) $\chi(a)=0$ *dacă* $(a, m)\neq 1$,

(*B*) $\chi(1)\neq 0$,

(*C*) $\chi(ab)=\chi(a)\ \chi(b)$,

(*D*) $\chi(a)=\chi(b)$ *dacă* $a\equiv b \pmod m$.

Observație. Proprietatea (*C*) ne arată că funcția caracter modulo m este total-multiplicativă.

Exemple de caractere modulo m.

(1) *Pentru orice număr întreg m funcția notată cu χ_1 definită prin*

$$\chi_1(a)=0 \text{ dacă } (a, m)\neq 1,$$
$$\chi_1(a)=1 \text{ dacă } (a, m)\equiv 1$$

este caracter modulo m. Această funcție se numește *caracter principal modulo m.*

Demonstrație.

(*A*) $\chi_1(a)=0$ dacă $(a, m)\neq 1$, datorită felului în care este definită funcția χ_1 ;

(*B*) $\chi_1(1)\neq 0$, deoarece $(1, m)\equiv 1$ și deci $\chi_1(1)=1$;

(*C*) $\chi_1(ab)=\chi_1(a)\ \chi_1(b)$, deoarece dacă $(ab, m)\neq 1$ rezultă $(a, m)\neq 1$ sau $(b, m)\neq 1$ și deci $\chi_1(ab)=0$ și în același timp $\chi_1(a)=0$ sau $\chi_1(b)=0$ adică $\chi_1(a)\ \chi_1(b)=0$, iar dacă $(ab, m)\equiv 1$ rezultă $(a, m)\equiv 1$ și $(b, m)\equiv 1$ și deci $\chi_1(ab)=1$ și în același timp $\chi_1(a)=\chi_1(b)=1$;

(*D*) $\chi_1(a)=\chi_1(b)$ dacă $a\equiv b \pmod m$, deoarece din $a\equiv b \pmod m$ și $(a, m)\neq 1$ rezultă $(b, m)\neq 1$ și deci $\chi_1(a)=\chi_1(b)=0$, iar dacă $(a, m)\equiv 1$, din $a\equiv b \pmod m$ rezultă $(b, m)\equiv 1$ și deci $\chi_1(a)=\chi_1(b)=1$.

(2) *Pentru $m=0$ funcția χ definită prin*

$$\chi(a)=0 \text{ dacă } a\neq \pm 1,$$
$$\chi(1)=1,\ \chi(-1)=-1$$

este caracter modulo m.

Demonstrație.

(*A*) $\chi(a)=0$ dacă $(a, 0)\neq 1$, deoarece din $(a, 0)\neq 1$ rezultă $a\neq \pm 1$.

(*B*) $\chi(1)\neq 0$, deoarece $\chi(1)=1$.

(*C*) $\chi(ab)=\chi(a)\ \chi(b)$, deoarece dacă $ab\neq \pm 1$ rezultă $a\neq \pm 1$ sau $b\neq \pm 1$ și deci $\chi(ab)=0$ și în același timp $\chi(a)=0$ sau $\chi(b)=0$ adică $\chi(a)\ \chi(b)=0$, iar dacă $ab=\pm 1$ atunci pentru $ab=1$ avem $a=b=1$ sau $a=b=-1$, iar pentru $ab=-1$ avem $a=1$, $b=-1$ sau $a=-1$, $b=1$ și deci $\chi(1)=\chi(1)\chi(1)=\chi(-1)\chi(-1)$, $\chi(-1)=\chi(1)\ \chi(-1)=\chi(-1)\ \chi(1)$, deoarece $\chi(1)=1$, $\chi(-1)=-1$.

(*D*) $\chi(a)=\chi(b)$ dacă $a\equiv b \pmod 0$, deoarece din $a\equiv b \pmod 0$ rezultă $a=b$.

(3) *Dacă m are un divizor n care admite o rădăcină primitivă g modulo n, atunci funcția χ definită prin*

$$\chi(a)=0 \text{ dacă } (a, m)\neq 1,$$
$$\chi(a)=\rho^{\gamma} \text{ dacă } (a, m)\equiv 1,$$

unde γ este orice număr întreg definit prin $a\equiv g^{\gamma} \pmod n$, iar ρ este o rădăcină primitivă a ecuației $x^{\varphi(n)}=1$, este caracter modulo m.

Demonstrație.

(*A*) $\chi(a)=0$ dacă $(a, m)\neq 1$ datorită felului în care este definită funcția χ.

(*B*) $\chi(1)\neq 0$, deoarece $(1, m)\cong 1$ și $1\equiv g^0 \pmod n$, deci $\chi(1)=\rho^0=1\neq 0$.

(*C*) $\chi(ab)=\chi(a)\,\chi(b)$, deoarece dacă $(ab, m)\not\cong 1$ rezultă $(a, m)\not\cong 1$ sau $(b, m)\not\cong 1$ și deci $\chi(ab)=0$ și în același timp $\chi(a)=0$ sau $\chi(b)=0$ adică $\chi(a)\,\chi(b)=0$, iar dacă $(ab, m)\cong 1$ rezultă $(a, m)\cong 1$ și $(b, m)\cong 1$ de unde rezultă că $(ab, n)\cong 1$, $(a, n)\cong 1$, $(b, n)\cong 1$, deoarece n este un divizor al lui m, așa că putem scrie $ab\equiv g^{\gamma_{ab}} \pmod n$, $a\equiv g^{\gamma_a} \pmod n$, $b\equiv g^{\gamma_b} \pmod n$, de unde deducem $\gamma_{ab}\equiv\gamma_a+\gamma_b \pmod{\varphi(n)}$, deci $\chi(ab)=\rho^{\gamma_{ab}}=\rho^{\gamma_a+\gamma_b+k\varphi(n)}=\rho^{\gamma_a}\rho^{\gamma_b}(\rho^{\varphi(n)})^k=\chi(a)\,\chi(b)$.

(*D*) $\chi(a)=\chi(b)$ dacă $a\equiv b \pmod m$, deoarece din $a\equiv b \pmod m$ și $(a, m)\not\cong 1$ rezultă $(b, m)\not\cong 1$ și deci $\chi(a)=0$, $\chi(b)=0$, iar dacă $(a, m)\cong 1$, din $a\equiv b \pmod m$ și $n|m$ rezultă $(a, n)\cong 1$ și $a\equiv b \pmod n$, așa că putem scrie $a\equiv g^{\gamma} \pmod n$ și deducem $b\equiv g^{\gamma} \pmod n$ și $(b, m)\cong 1$, deci $\chi(a)=\rho^{\gamma}$, $\chi(b)=\rho^{\gamma}$.

(4) *Dacă m are ca divizor pe $n=2^\alpha$ cu $\alpha\geqslant 3$, atunci funcția χ definită prin*

$$\chi(a)=0 \text{ dacă } (a, m)\not\cong 1,$$
$$\chi(a)=(-1)^{\gamma} \text{ dacă } (a, m)\cong 1,$$

unde γ este orice număr întreg definit prin $a\equiv(-1)^{\gamma}5^{\gamma_0} \pmod{2^\alpha}$ este caracter modulo m.

Demonstrație.

(*A*) $\chi(a)=0$ dacă $(a, m)\not\cong 1$ datorită felului în care este definită funcția χ.

(*B*) $\chi(1)\neq 0$, deoarece $(1, m)\cong 1$ și $1\equiv(-1)^0 5^0 \pmod{2^\alpha}$ deci $\chi(1)=(-1)^0=1\neq 0$.

(*C*) $\chi(ab)=\chi(a)\,\chi(b)$, deoarece dacă $(ab, m)\not\cong 1$ rezultă $(a, m)\not\cong 1$ sau $(b, m)\not\cong 1$ și deci $\chi(ab)=0$ și în același timp $\chi(a)=0$ sau $\chi(b)=0$ adică $\chi(a)\,\chi(b)=0$, iar dacă $(ab, m)\cong 1$ rezultă $(a, m)\cong 1$ și $(b,m)\cong 1$ de unde rezultă că $(ab, 2^\alpha)\cong 1$, $(a, 2^\alpha)\cong 1$, $(b, 2^\alpha)\cong 1$, deoarece 2^α este un divizor al lui m, așa că putem scrie $ab\equiv(-1)^{\gamma_{ab}}5^{\gamma_{0ab}} \pmod{2^\alpha}$, $a\equiv(-1)^{\gamma_a}5^{\gamma_{0a}} \pmod{2^\alpha}$, $b\equiv(-1)^{\gamma_b}5^{\gamma_{0b}} \pmod{2^\alpha}$, de unde deducem $\gamma_{0ab}\equiv\gamma_{0a}+\gamma_{0b} \pmod{\frac{1}{2}\varphi(2^\alpha)}$, deci $\chi(ab)=\rho^{\gamma_{0ab}}=\rho^{\gamma_{0a}+\gamma_{0b}+\frac{k}{2}\varphi(2^\alpha)}=\rho^{\gamma_{0a}}\rho^{\gamma_{0b}}(\rho^{\frac{1}{2}\varphi(2^\alpha)})^k=\chi(a)\,\chi(b)$.

(*D*) $\chi(a)=\chi(b)$ dacă $a\equiv b \pmod m$, deoarece din $a\equiv b \pmod m$ și $(a, m)\not\cong 1$ rezultă $(b, m)\not\cong 1$ și deci $\chi(a)=0$, $\chi(b)=0$, iar dacă $(a, m)\cong 1$, din $a\equiv b \pmod m$ și $2^\alpha|m$ rezultă $(a, 2^\alpha)\cong 1$ și $a\equiv b \pmod{2^\alpha}$, așa că putem scrie $a\equiv(-1)^{\gamma}5^{\gamma_0} \pmod{2^\alpha}$ și deducem $b\equiv(-1)^{\gamma}5^{\gamma_0} \pmod{2^\alpha}$ și $(b, m)\cong 1$, deci $\chi(a)=\rho^{\gamma_0}$, $\chi(b)=\rho^{\gamma_0}$.

(5) *Dacă m are ca divizor pe $n=2^\alpha$ cu $\alpha\geqslant 3$, atunci funcția χ definită prin*

$$\chi(a)=0 \text{ dacă } (a, m)\not\cong 1,$$
$$\chi(a)=\rho^{\gamma_0} \text{ dacă } (a, m)\cong 1,$$

unde γ_0 este orice număr întreg definit prin $a\equiv(-1)^{\gamma}5^{\gamma_0} \pmod{2^\alpha}$, iar ρ este o rădăcină primitivă a ecuației $x^{\frac{1}{2}\varphi(2^\alpha)}=1$, este caracter modulo m.

Demonstrație.

(*A*) $\chi(a)=0$ dacă $(a, m)\not\cong 1$ datorită felului în care este definită funcția χ.

(*B*) $\chi(1)\neq 0$, deoarece $(1, m)\cong 1$ și $1\equiv(-1)^0 5^0 \pmod{2^\alpha}$ deci $\chi(1)=\rho^0=1\neq 0$.

(*C*) $\chi(ab)=\chi(a)\,\chi(b)$, deoarece dacă $(ab, m)\not\cong 1$ rezultă $(a, m)\not\cong 1$ sau $(b, m)\not\cong 1$ și deci $\chi(ab)=0$ și în același timp $\chi(a)=0$ sau $\chi(b)=0$ adică $\chi(a)\,\chi(b)=0$, iar dacă $(ab, m)\cong 1$ rezultă $(a, m)\cong 1$ și $(b, m)\cong 1$ de unde rezultă că $(ab, 2^\alpha)\cong 1$, $(a,2^\alpha)\cong 1$, $(b, 2^\alpha)\cong 1$, deoarece 2^α este un divizor al lui m, așa că putem scrie $ab\equiv(-1)^{\gamma_{ab}}5^{\gamma_{0ab}} \pmod{2^\alpha}$, $a\equiv(-1)^{\gamma_a}5^{\gamma_{0a}} \pmod{2^\alpha}$, $b\equiv(-1)^{\gamma_b}5^{\gamma_{0b}} \pmod{2^\alpha}$, de unde deducem $\gamma_{0ab}\equiv\gamma_{0a}+\gamma_{0b} \pmod{\frac{1}{2}\varphi(2^\alpha)}$, deci $\chi(ab)=\rho^{\gamma_{0ab}}=\rho^{\gamma_{0a}+\gamma_{0b}+\frac{k}{2}\varphi(2^\alpha)}=\rho^{\gamma_{0a}}\rho^{\gamma_{0b}}(\rho^{\frac{1}{2}\varphi(2^\alpha)})^k=\chi(a)\,\chi(b)$.

(*D*) $\chi(a)=\chi(b)$ dacă $a\equiv b \pmod m$, deoarece din $a\equiv b \pmod m$ și $(a, m)\not\cong 1$ rezultă $(b, m)\not\cong 1$ și deci $\chi(a)=0$, $\chi(b)=0$, iar dacă $(a, m)\cong 1$, din $a\equiv b \pmod m$ și $2^\alpha|m$ rezultă $(a, 2^\alpha)\cong 1$ și $a\equiv b \pmod{2^\alpha}$, așa că putem scrie $a\equiv(-1)^{\gamma}5^{\gamma_0} \pmod{2^\alpha}$ și deducem $b\equiv(-1)^{\gamma}5^{\gamma_0} \pmod{2^\alpha}$ și $(b, m)\cong 1$, deci $\chi(a)=\rho^{\gamma_0}$, $\chi(b)=\rho^{\gamma_0}$.

10.2. Cîteva proprietăți ale caracterelor modulo m

(1) $\chi(1)=1$ *pentru orice caracter χ modulo m.*

Demonstrație. Conform proprietății (*C*) avem

$$\chi(1\cdot 1)=\chi(1)\,\chi(1)$$

deci $\chi(1)=\chi(1)\,\chi(1)$. Această egalitate este o egalitate între numere complexe. Datorită proprietății (B) avem $\chi(1)\neq 0$ și atunci obținem, prin simplificare, că $1=\chi(1)$.

(2) *Dacă* $(a, m)\cong 1$, *atunci* $(\chi(a))^{\varphi(m)}=1$ *pentru orice caracter* χ *modulo* m.

Demonstrație. Conform proprietății (C) avem

$$\chi(a^{\varphi(m)})=\chi(\underbrace{a\cdot\ldots\cdot a}_{\text{de }(m)\text{ ori}})=\chi(\underbrace{a)\cdot\ldots\cdot\chi(a}_{\text{de }\varphi(m)\text{ ori}})=(\chi(a))^{\varphi(m)}.$$

Conform proprietății (D), din $a^{\varphi(m)}\equiv 1 \pmod m$, care exprimă teorema lui Euler, deoarece $(a, m)\cong 1$, obținem $\chi(a^{\varphi(m)})=\chi(1)=1$, deci

$$1=(\chi(a))^{\varphi(m)}.$$

Observație. Această proprietate exprimă faptul că valorile caracterului χ modulo m pentru numere întregi a prime cu modulul m sînt rădăcinile unității de gradul $\varphi(m)$, adică sînt rădăcinile ecuației

$$x^{\varphi(m)}=1.$$

(3) *Numărul caracterelor modulo* m *este finit.*

Demonstrație. Datorită proprietăților (D) și (A), un caracter modulo m, notat cu χ, este definit prin sistemul de valori

$$\chi(c_1),\ \chi(c_2),\ \ldots,\ \chi(c_{\varphi(m)}),$$

unde $c_1, c_2, \ldots c_{\varphi(m)}$ este un sistem redus de resturi modulo m. Însă $\chi(c_i)$, unde $i=1, 2, \ldots, \varphi(m)$, poate fi egală numai cu una din cele $\varphi(m)$ rădăcini ale ecuației $x^{\varphi(m)}=1$ din cauză că $(c_i, m)\cong 1$, c_i făcînd parte dintr-un sistem redus de resturi modulo m. Deci $\chi(c_1)$ poate avea numai $\varphi(m)$ valori. La fiecare valoare a lui $\chi(c_1)$ putem avea pentru $\chi(c_2)$ numai $\varphi(m)$ valori, deci sistemul $\chi(c_1)$, $\chi(c_2)$ poate avea numai $\varphi(m)\,\varphi(m)=(\varphi(m))^2$ valori. La fiecare sistem $\chi(c_1)$, $\chi(c_2)$ putem avea pentru $\chi(c_3)$ numai $\varphi(m)$ valori, deci sistemul $\chi(c_1)$, $\chi(c_2)$, $\chi(c_3)$ poate avea numai $(\varphi(m))^2\,\varphi(m)=(\varphi(m))^3$ valori. Continuînd raționamentul în acest mod, ajungem la concluzia că sistemul $\chi(c_1)$, $\chi(c_2)$, $\ldots$, $\chi(c_{\varphi(m)})$ poate avea numai $\varphi(m)^{\varphi(m)}$ valori. Deci numărul caracterelor modulo m este cel mult egal cu $\varphi(m)^{\varphi(m)}$ deci este finit.

(4) *Dacă* χ_i, χ_j *sînt caractere modulo* m, *atunci produsul lor este caracter modulo* m.

Demonstrație.

Să notăm cu χ_{ij} funcția obținută făcînd produsul funcțiilor χ_i, χ_j.

(A) $\chi_{ij}(a)=0$ dacă $(a, m)\not\cong 1$, deoarece $\chi_i(a)=0$, $\chi_j(a)=0$, iar $\chi_{ij}(a)=\chi_i(a)\,\chi_j(a)$.

(B) $\chi_{ij}(1)\neq 0$, deoarece $\chi_{ij}(1)=\chi_i(1)\,\chi_j(1)$, iar $\chi_i(1)\neq 0$, $\chi_j(1)\neq 0$.

(C) $\chi_{ij}(ab)=\chi_{ij}(a)\,\chi_{ij}(b)$, deoarece $\chi_{ij}(ab)=\chi_i(ab)\chi_j(ab)=$
$=(\chi_i(a)\,\chi_i(b))\,(\chi_j(a)\chi_j(b))=(\chi_i(a)\,\chi_j(a))\,(\chi_i(b)\,\chi_j(b))=\chi_{ij}(a)\,\chi_{ij}(b)$.

(D) $\chi_{ij}(a)=\chi_{ij}(b)$ dacă $a\equiv b \pmod m$, deoarece $\chi_i(a)=\chi_i(b)$, $\chi_j(a)=\chi_j(b)$ deci $\chi_i(a)\,\chi_j(a)=\chi_i(b)\,\chi_j(b)$ adică $\chi_{ij}(a)=\chi_{ij}(b)$.

(5) *Dacă* $\chi_1, \chi_2, \ldots, \chi_k$ *sînt toate caracterele modulo* m, *atunci* $\chi_{s1}, \chi_{s2}, \ldots, \chi_{sk}$ *sînt, de asemenea, toate caracterele modulo* m, *unde* χ_{si} *este produsul caracterelor* χ_s *și* χ_i.

Demonstrație. Mai întîi χ_{si} pentru $i=1, 2, \ldots, k$ sînt caractere modulo m. Apoi numărul lor este k și ele sînt distincte două cîte două, deoarece dacă am avea $\chi_{si}=\chi_{sj}$ cu $i\neq j$, atunci pentru a prim cu m, din $\chi_{si}(a)=\chi_{sj}(a)$, adică din $\chi_s(a)\,\chi_i(a)=\chi_s(a)\,\chi_j(a)$ am deduce $\chi_i(a)=\chi_j(a)$, pentru că $\chi_s(a)\neq 0$, ceea ce rezultă din $(\chi_s(a))^{\varphi(m)}=1$, care împreună cu $\chi_i(a)=\chi_j(a)$ pentru a neprim cu m, din cauză că $\chi_i(a)=0$, $\chi_j(a)=0$, ne conduce la o contradicție, avînd în vedere că $\chi_i\neq\chi_j$ cu $i\neq j$.

(6) *Fiind dat un număr întreg* d *pentru care* $(d, m)\cong 1$ *și* $d\not\equiv 1 \pmod m$, *există un caracter* χ *modulo* m *astfel încît* $\chi(d)\neq 1$.

Demonstrație.

Dacă $m=0$, atunci numai pentru $d=\pm 1$ avem $(d, m)\cong 1$. Pentru $m=0$, relația de congruență se transformă în relația de egalitate și deci numai pentru $d=-1$ avem $d\neq 1$. Trebuie să arătăm că există un caracter χ modulo 0 astfel încît $\chi(-1)\neq 1$. Acest lucru l-am dovedit cînd am dat exemplul (2) de caracter modulo 0, unde avem $\chi(-1)=-1$ deci $\chi(-1)\neq 1$.

Dacă $m=\pm 1$, atunci pentru orice număr întreg a avem $a\equiv 1 \pmod{\pm 1}$ și deci nu se pune problema.

Dacă $m\neq 0$, $m\neq\pm 1$, putem scrie

$$m=\varepsilon p_1^{\alpha_1}p_2^{\alpha_2}\ldots\ p_r^{\alpha_r},$$

unde $\varepsilon=\pm 1$, $p_1, p_2, \ldots, p_r$ sînt numere prime pozitive diferite două cîte două, iar $\alpha_1, \alpha_2, \ldots, \alpha_r$ sînt numere naturale.

Să luăm numărul întreg d care ne interesează și pentru care

$$(d,\ m)\cong 1,\ d\not\equiv 1 \pmod m.$$

Din cauză că $d\not\equiv 1 \pmod m$ înseamnă că există un indice i cu $1\leqslant i\leqslant r$ astfel, încît

$$d\not\equiv 1 \pmod{p_i^{\alpha_i}},$$

deoarece dacă $d\equiv 1 \pmod{p_j^{\alpha_j}}$ pentru orice $j=1,\ 2,\ \ldots,\ r$ atunci $d\equiv 1 \pmod m$, avînd în vedere că $p_j^{\alpha}\mid d-1$ pentru orice $j=1,\ 2,\ \ldots,\ r$, iar m este cel mai mic multiplu comun al lui $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_r^{\alpha_r}$, ceea ce este contradictoriu. Apoi avem și $(d,\ p_i^{\alpha_i})\cong 1$ din cauză că $(d,\ m)\cong 1$, iar $p_i^{\alpha_i}\mid m$.

Cazul I. $p_i^{\alpha_i}$ este un modul pentru care există rădăcini primitive. Deoarece $(d,\ p_i^{\alpha_i})\cong 1$ și $d\not\equiv 1 \pmod{p_i^{\alpha}}$, înseamnă că $d\equiv g^{\gamma_d} \pmod{p_i^{\alpha_i}}$ cu $\gamma_d\not\equiv 0$, $0\leqslant\gamma_d\leqslant\varphi(p_i^{\alpha_i})-1$, g fiind o rădăcină primitivă modulo $p_i^{\alpha_i}$. Dacă luăm caracterul χ modulo m dat în exemplul (3), unde punem $n=p_i^{\alpha_i}$, obținem $\chi(d)=\rho^{\gamma_d}\neq 1$, deoarece $0<\gamma_d<\varphi(p_i^{\alpha_i})$, ρ fiind rădăcină primitivă a ecuației $x^{\varphi(p_i\alpha_i)}=1$.

Cazul II. $p_i^{\alpha_i}$ este un modul pentru care nu există rădăcini primitive. Asta înseamnă că $p_i=\pm 2$, iar $\alpha_i\geqslant 3$, deoarece în caz contrar, adică în cazul cînd $p_i\neq\pm 2$ sau $p_i=\pm 2$, dar $0\leqslant\alpha_i<3$, există rădăcini primitive modulo $p_i^{\alpha_i}$. Deoarece $(d,\ p_i^{\alpha_i})\cong 1$, adică $(d,\ 2^{\alpha_i})\cong 1$ și $d\not\equiv 1 \pmod{2^{\alpha_i}}$, înseamnă că $d\equiv(-1)^{\gamma_{1d}}5^{\gamma_{0d}} \pmod{2^{\alpha_i}}$, unde $\gamma_d\not\equiv 0$ sau $\gamma_{0d}\not\equiv 0$ și $0\leqslant\gamma_d\leqslant 1$, $0\leqslant\gamma_{0d}\leqslant\frac{1}{2}\varphi(2^{\alpha})-1$.

Subcazul II_1. În $d\equiv(-1)^{\gamma_{1d}}5^{\gamma_{0d}} \pmod{2^{\alpha_i}}$ avem $\gamma_{1d}\not\equiv 0$. Dacă luăm caracterul χ modulo m dat în exemplul (4), obținem $\chi(d)=(-1)^{\gamma_{1d}}=-1\neq 1$, deoarece $\gamma_{1d}\not\equiv 0$ și $0\leqslant\gamma_{1d}\leqslant 1$ deci $\gamma_{1d}=1$.

Subcazul II_2. În $d\equiv(-1)^{\gamma_{1d}}5^{\gamma_{0d}} \pmod{2^{\alpha_i}}$ avem $\gamma_{1d}=0$. Atunci $\gamma_{0d}\not\equiv 0$, deoarece dacă și $\gamma_{0d}=0$ atunci $d\equiv 1 \pmod{2^{\alpha_i}}$, ceea ce contrazice $d\not\equiv 1 \pmod{p_i^{\alpha_i}}$. Dacă luăm caracterul χ modulo m dat în exemplul (5), obținem $\chi(d)=\rho^{\gamma_{0d}}\neq 1$, deoarece $0<\gamma_{0d}<\frac{1}{2}\varphi(2^{\alpha_i})$, ρ fiind rădăcină primitivă a ecuației $x^{\frac{1}{2}\varphi(2^{\alpha_i})}=1$.

10.3. Proprietățile caracterelor modulo m în legătură cu sumele care se fac cu ele

$$(1)\quad \sum_a \chi(a)=\begin{cases}\varphi(m) & \text{dacă } \chi=\chi_1,\\ 0 & \text{dacă } \chi\neq\chi_1,\end{cases}$$

unde suma este extinsă la un sistem complet de resturi modulo m.

Demonstrație. Dacă $\chi=\chi_1$ ținem seama de $\sum_a \chi_1(a)=\sum_c \chi_1(c)=$ $=\underbrace{1+\ldots+1}_{\text{de }\varphi(m)\text{ ori}}=\varphi(m)$, unde suma $\sum_c \chi_1(c)$ este extinsă la un sistem redus de resturi modulo m, deoarece dacă $(a,\ m)\not\cong 1$ atunci $\chi_1(a)=0$, iar dacă $(a,\ m)\cong 1$ atunci $\chi_1(a)=1$.

Dacă $\chi\neq\chi_1$ înseamnă că există un număr întreg b prim cu m astfel încît $\chi(b)\neq 1$, deoarece dacă pentru orice număr întreg b prim cu m avem $\chi(b)=1$, atunci $\chi=\chi_1$, ceea ce este contradictoriu. Ținînd seama de faptul că dacă a parcurge un sistem complet de resturi modulo m, atunci și ab parcurge un sistem complet de resturi modulo m, din cauză că $(b,\ m)\cong 1$, înseamnă că

$$\sum_a \chi(a)=\sum_a \chi(ab).$$

Dar $\sum_a \chi(ab)=\sum_a \chi(a)\,\chi(b)=\chi(b)\sum_a \chi(a)$. Deci

$$\sum_a \chi(a)=\chi(b)\sum_a \chi(a),$$

adică $(1-\chi(b))\sum_a \chi(a)=0$ și cum $\chi(b)\neq 1$ rezultă $\sum_a \chi(a)=0$.

$$(2)\quad \sum_j \chi_j(a)=\begin{cases}Z & \text{dacă } a\equiv 1 \pmod m,\\ 0 & \text{dacă } a\not\equiv 1 \pmod m,\end{cases}$$

unde suma este extinsă la toate caracterele modulo m, Z fiind numărul acestor caractere.

Demonstrație.

În cazul cînd $a\equiv 1 \pmod m$ avem $\chi_j(a)=\chi_j(1)=1$ deci, în acest caz,

$$\sum_j \chi_j(a)=\underbrace{1+\ldots+1}_{\text{de }Z\text{ ori}}=Z.$$

În cazul cînd $a\not\equiv 1 \pmod m$ putem avea $(a,\ m)\not\cong 1$ sau $(a,\ m)\cong 1$.

Dacă $(a, m)\not\cong 1$ atunci $\chi_j(a)=0$ deci, în acest caz

$$\sum_j \chi_j(a)=0.$$

Dacă $(a, m)\cong 1$, cum $a\not\equiv 1 \pmod m$ rezultă că există un caracter χ_s modulo m astfel încît $\chi_s(a)\neq 1$. Ținînd seama de faptul că dacă χ_j parcurge toate caracterele modulo m, atunci și χ_{sj} parcurge toate caracterele modulo m, unde χ_{sj} este produsul caracterelor χ_s și χ_j rezultă că

$$\sum_j \chi_j(a)=\sum_j \chi_{sj}(a).$$

Dar $\sum_j \chi_{sj}(a)=\sum_j \chi_s(a)\ \chi_j(a)=\chi_s(a)\sum_j \chi_j(a)$. Deci

$$\sum_j \chi_j(a)=\chi_s(a)\sum_j \chi_j(a),$$

adică $(1-\chi_s(a))\sum_j \chi_j(a)=0$ și cum $\chi_s(a)\neq 1$ rezultă $\sum_j \chi_j(a)=0$.

(3) $Z=\varphi(m)$, *unde* Z *este numărul caracterelor modulo* m.

Demonstrație.

$$Z=\sum_{a\equiv 1 \pmod m} \sum_j \chi_j(a) \quad \text{și} \quad 0=\sum_{a\not\equiv 1 \pmod m} \sum_j \chi_j(a).$$

Făcînd pe a să parcurgă un sistem complet de resturi modulo m, vom avea $a\equiv 1 \pmod m$ numai pentru un singur a din sistemul complet de resturi considerat și de aceea

$$Z=\sum_a \sum_j \chi_j(a),$$

prima sumă fiind extinsă la un sistem complet de resturi modulo m. Schimbînd ordinea de sumare avem

$$Z=\sum_j \sum_a \chi_j(a).$$

Dar $\sum_a \chi_j(a)=\varphi(m)$ numai dacă $\chi_j=\chi_1$, unde χ_1 este caracter principal modulo m. În toate celelalte cazuri avem $\sum_a \chi_j(a)=0$, deci

$$Z=\sum_a \chi_1(a)=\varphi(m).$$

(4) *Dacă* $(t, m)\cong 1$, *atunci*

$$\sum_j \chi_j(a)\ \overline{\chi_j(t)}=\begin{cases}\varphi(m) \text{ dacă } a\equiv t \pmod m,\\ 0 \text{ dacă } a\not\equiv t \pmod m,\end{cases}$$

unde $\overline{\chi_j(t)}$ *este complexul conjugat al lui* $\chi_j(t)$, *suma fiind extinsă la toate caracterele modulo* m.

Demonstrație. Deoarece $(t, m)\cong 1$, congruența

$$xt\equiv 1 \pmod m$$

admite soluții. Fie s un număr întreg astfel încît

$$st\equiv 1 \pmod m.$$

Avem $\chi_j(st)=\chi_j(1)=1$, deci $\chi_j(s)\ \chi_j(t)=1$. Rezultă că $\overline{\chi_j(t)}=\frac{1}{\chi_j(t)}=\chi_j(s)$. Avem $\overline{\chi_j(t)}=\frac{1}{\chi_j(t)}$, deoarece $(\chi_j(t))^{\varphi(m)}=1$, deci $\overline{(\chi_j(t))^{\varphi(m)}}=\overline{1}$, adică $(\overline{\chi_j(t)})^{\varphi(m)}=1$ de unde rezultă $(\overline{\chi_j(t)})^{\varphi(m)}(\chi_j(t))^{\varphi(m)}=1$ sau $(\chi_j(t)\overline{\chi_j(t)})^{\varphi(m)}=1$. Singura rădăcină reală și pozitivă a ecuației $x^{\varphi(m)}=1$ fiind 1 avem $\chi_j(t)\ \overline{\chi_j(t)}=1$, deci $\overline{\chi_j(t)}=\frac{1}{\chi_j(t)}$.

Avem deci

$$\sum_j \chi_j(a)\overline{\chi_j(t)}=\sum_j \chi_j(a)\ \chi_j(s)=\sum_j \chi_j(as)=\begin{cases}\varphi(m) \text{ dacă } as\equiv 1 \pmod m,\\ 0 \text{ dacă } as\not\equiv 1 \pmod m.\end{cases}$$

Dar din $as\equiv 1 \pmod m$ și $st\equiv 1 \pmod m$ deducem $ast\equiv t \pmod m$ deci $a\equiv t \pmod m$ și reciproc din $a\equiv t \pmod m$ și $st\equiv 1 \pmod m$ deducem $as\equiv st \pmod m$ deci $as\equiv 1 \pmod m$, deci din $as\not\equiv 1 \pmod m$ se deduce $a\not\equiv t \pmod m$ și reciproc din $a\not\equiv t \pmod m$ se deduce $as\not\equiv 1 \pmod m$. Cu acestea proprietatea enunțată este demonstrată.

10.4. Simbolul lui Legendre

Definiție. *Simbolul lui Legendre este o funcție numerică, care se notează cu* $\left(\frac{a}{p}\right)$, *unde* p *este un număr prim impar, iar* a *un număr întreg, definită prin*

$$\left(\frac{a}{p}\right)=\begin{cases}0 \text{ dacă } p\mid a,\\ 1 \text{ dacă } p\nmid a, \text{ iar } a \text{ este rest pătratic modulo } p,\\ -1 \text{ dacă } p\nmid a, \text{ iar } a \text{ este nerest pătratic modulo } p.\end{cases}$$

Teoremă. *Simbolul lui Legendre* $\left(\frac{a}{p}\right)$ *este un caracter modulo* p.

Demonstrație.

$(A)\left(\frac{a}{p}\right)=0$ dacă $(a, p)\not\cong 1$, deoarece $\left(\frac{a}{p}\right)=0$ dacă $p|a$, iar $p|a$ este echivalent cu $(a, p)\not\cong 1$, p fiind un număr prim.

$(B)\left(\frac{1}{p}\right)\neq 0$ din cauză că $p\nmid 1$, iar 1 este rest pătratic modulo p, deci $\left(\frac{1}{p}\right)=1\neq 0$.

$(C)\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. În adevăr, dacă $p|ab$ atunci $p|a$ sau $p|b$ deci $\left(\frac{ab}{p}\right)=0$ și în același timp $\left(\frac{a}{p}\right)=0$ sau $\left(\frac{b}{p}\right)=0$, adică $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)=0$, de unde $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. Dacă $p\nmid ab$ atunci $p\nmid a$ și $p\nmid b$. Relațiile $p\nmid ab$, $p\nmid a$, $p\nmid b$ sînt echivalente respectiv cu relațiile $(ab, p)\cong 1$, $(a, p)\cong 1$, $(b, p)\cong 1$. Fie g o rădăcină primitivă modulo p. Atunci

$$a \equiv g^{\text{ind } a} \pmod p,$$
$$b \equiv g^{\text{ind } b} \pmod p,$$
$$ab \equiv g^{\text{ind } ab} \pmod p,$$

unde $\text{ind}(ab)\equiv\text{ind } a+\text{ind } b \pmod{\varphi(p)}$. Din cauză că $\varphi(p)=|p|-1$, iar p este impar, se deduce că $2|\varphi(p)$, deci

$$\text{ind } (ab)\equiv\text{ind } a+\text{ind } b \pmod 2.$$

Fiind vorba de resturi și neresturi pătratice modulo p, înseamnă că este vorba de congruențe de tipul

$$x^2\equiv a \pmod p.$$

Avem $(2, \varphi(p))\cong 2$, deci condiția necesară și suficientă ca a să fie rest pătratic modulo p este ca $2|\text{ind } a$. Asta înseamnă că dacă a este rest pătratic modulo p și b este rest pătratic modulo p, avem $2|\text{ind } a$, $2|\text{ind } b$, deci $2|\text{ind } (ab)$, ceea ce rezultă din $\text{ind } (ab)\equiv\text{ind } a+\text{ind } b \pmod 2$, deci $\left(\frac{a}{p}\right)=1$, $\left(\frac{b}{p}\right)=1$, $\left(\frac{ab}{p}\right)=1$ și deci $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;

dacă a este nerest pătratic modulo p și b este rest pătratic modulo p, avem $2\nmid\text{ind } a$, $2|\text{ind } b$, deci $2\nmid\text{ind } a+\text{ind } b$, de unde rezultă $2\nmid\text{ind } (ab)$, deci $\left(\frac{a}{p}\right)=-1$, $\left(\frac{b}{p}\right)=1$, $\left(\frac{ab}{p}\right)=-1$, și deci $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;

dacă a este rest pătratic modulo p și b este nerest pătratic modulo p, atunci avem o situație analoagă cu cea precedentă și deci $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;

dacă a este nerest pătratic modulo p și b este nerest pătratic modulo p, avem $2\nmid\text{ind } a$, $2\nmid\text{ind } b$, de unde rezultă $2|\text{ind } a+\text{ind } b$, deci $2|\text{ind } (ab)$, deci $\left(\frac{a}{p}\right)=-1$, $\left(\frac{b}{p}\right)=-1$, $\left(\frac{ab}{p}\right)=1$ și deci $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

$(D)\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$ dacă $a\equiv b \pmod p$. În adevăr, dacă $p|a$ atunci din $a\equiv b \pmod p$ rezultă $p|b$, deci $\left(\frac{a}{p}\right)=0$, $\left(\frac{b}{p}\right)=0$ și deci $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$.

Dacă $p\nmid a$ atunci din $a\equiv b \pmod p$ rezultă $p\nmid b$. Relațiile $p\nmid a$, $p\nmid b$ fiind echivalente respectiv cu $(a, p)\cong 1$, $(b, p)\cong 1$, înseamnă că $\text{ind } a\equiv\text{ind } b \pmod{\varphi(p)}$ cu $a\equiv g^{\text{ind } a} \pmod p$, $b\equiv g^{\text{ind } b} \pmod p$, unde g este o rădăcină primitivă modulo p. Din $\text{ind } a\equiv\text{ind } b \pmod{\varphi(p)}$ rezultă $\text{ind } a\equiv\text{ind } b \pmod 2$. Dacă a este rest pătratic modulo p, atunci $2|\text{ind } a$, deci și $2|\text{ind } b$, deci $\left(\frac{a}{p}\right)=1$, $\left(\frac{b}{p}\right)=1$, adică $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$. Dacă a este nerest pătratic modulo p, atunci $2\nmid\text{ind } a$, deci și $2\nmid\text{ind } b$, deci $\left(\frac{a}{p}\right)=-1$, $\left(\frac{b}{p}\right)=-1$ și deci $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$.

Capitolul 11

RESTURI PĂTRATICE

11.1. Criterii ca un număr întreg a să fie rest pătratic modulo p unde p este un număr impar

(1) *Criteriul dat cu ajutorul rădăcinilor primitive modulo p. Condiția necesară și suficientă ca un număr întreg a, nedivizibil prin p, p fiind prim impar, să fie rest pătratic modulo p este ca*

$$2 | \text{ind } a.$$

Demonstrația acestui criteriu este un caz particular al demonstrației prin care se arată că $d|\text{ind } a$ este condiția necesară și suficientă ca un număr întreg a să fie rest de gradul n modulo m, a fiind prim cu m, modulul m admițînd rădăcini primitive modulo m, iar $d \cong (n, \varphi(m))$.

(2) *Criteriul lui Euler*:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{|p|-1}{2}} \pmod{p}.$$

Demonstrație. Am arătat că un număr întreg a prim cu m este rest de gradul n modulo m dacă și numai dacă

$$a^{\frac{c}{d}} \equiv 1 \pmod{m},$$

unde $m = \pm p^\beta$ sau $\pm 2p^\beta$, p fiind prim pozitiv impar, β număr natural, $c = \varphi(m)$, $d \cong (n, c)$, $d > 0$.

Particularizînd la resturile pătratice modulo p, avem $c = \varphi(p) = |p| - 1$, $d = 2$, deoarece $2 \cong (2, \varphi(p))$ și deci dacă $p \nmid a$, atunci a este rest pătratic modulo p dacă și numai dacă

$$a^{\frac{\varphi(p)}{2}} \equiv 1 \pmod{p}.$$

Apoi, conform teoremei lui Fermat, pentru orice a pentru care $p \nmid a$ avem

$$a^{\varphi(p)} \equiv 1 \pmod{p}.$$

Din cauză că $2 | \varphi(p)$ obținem $a^{\varphi(p)} - 1 = \left(a^{\frac{\varphi(p)}{2}} - 1\right)\left(a^{\frac{\varphi(p)}{2}} + 1\right)$, deci

$$\left(a^{\frac{\varphi(p)}{2}} - 1\right)\left(a^{\frac{\varphi(p)}{2}} + 1\right) \equiv 0 \pmod{p}.$$

Rezultă că $p \mid \left(a^{\frac{\varphi(p)}{2}} - 1\right)\left(a^{\frac{\varphi(p)}{2}} + 1\right)$. Dacă a este nerest pătratic modulo p, avem $a^{\frac{\varphi(p)}{2}} \not\equiv 1 \pmod{p}$, conform celor spuse mai sus, deci $p \nmid \left(a^{\frac{\varphi(p)}{2}} - 1\right)$ și cum p este prim, din $p \mid \left(a^{\frac{\varphi(p)}{2}} - 1\right)\left(a^{\frac{\varphi(p)}{2}} + 1\right)$ rezultă $p \mid a^{\frac{\varphi(p)}{2}} + 1$. Reciproc, dacă $p \mid a^{\frac{\varphi(p)}{2}} + 1$, atunci a este nerest pătratic modulo p, deoarece dacă a ar fi rest pătratic modulo p, am avea $p \mid a^{\frac{\varphi(p)}{2}} + 1$ și $a^{\frac{\varphi(p)}{2}} \equiv 1 \pmod{p}$, deci $a^{\frac{\varphi(p)}{2}} \equiv -1 \pmod{p}$ și $a^{\frac{\varphi(p)}{2}} \equiv 1 \pmod{p}$, deci $-1 \equiv 1 \pmod{p}$ sau $2 \equiv 0 \pmod{p}$ sau $p | 2$, ceea ce este contradictoriu, deoarece p este impar.

Am arătat deci că condiția necesară și suficientă ca un număr întreg a pentru care $p\nmid a$ să fie nerest pătratic este

$$a^{\frac{\varphi(p)}{2}} \equiv -1 \pmod{p}.$$

Deci în cazul cînd $p\nmid a$, rezultă că

$$\left(\frac{a}{p}\right) \equiv a^{\frac{\varphi(p)}{2}} \pmod{p}.$$

Și în cazul cînd $p|a$, congruență de mai sus este adevărată, deoarece în acest caz $\left(\frac{a}{p}\right)=0$, iar $a^{\frac{\varphi(p)}{2}} \equiv 0 \pmod{p}$.

(3) *Criteriul lui Gauss.*
Dacă $p\nmid a$ *atunci*

$$\left(\frac{a}{p}\right) = (-1)^{\lambda},$$

unde $\lambda = \sum_{i=1}^{\frac{|p|-1}{2}} \alpha_i$, *numerele* $\alpha_i (\alpha_i = 0$ *sau* $\alpha_i = 1, i = 1, \ldots, \frac{|p|-1}{2})$ *fiind definite prin intermediul congruenței* $ai \equiv (-1)^{\alpha_i} r_i \pmod{p}$ *în care numărul natural* r_i *satisface relația* $r_i < \frac{|p|}{2}$, *la valori distincte ale lui* i *corespunzînd valori distincte ale lui* r_i.

Demonstrație. Fiind dat numărul prim impar p, vom lua numerele naturale $1, 2, \ldots, \frac{|p|-1}{2}$. Să notăm cu i unul oarecare dintre aceste numere naturale. Avem $i < \frac{|p|}{2}$ și orice număr natural i care verifică relația $i < \frac{|p|}{2}$ este unul dintre numerele naturale $1, 2, \ldots, \frac{|p|-1}{2}$. Aplicînd teorema împărțirii întregi lui ai și p obținem

$$ai = pQ + R, \quad 0 \leqslant R < |p|.$$

Nu putem avea $R=0$, deoarece dacă $R=0$ avem $p|ai$ și cum $p\nmid a$ trebuie ca $p|i$, p fiind număr prim, ceea ce nu se poate din cauză că din $p|i$ și $i \neq 0$ rezultă $|p| < i$ pe cînd $i < \frac{|p|}{2} < |p|$.

Deci $0 < R < |p|$. Dacă $0 < R < \frac{|p|}{2}$, vom nota $R = r_i$ și vom avea

$$ai \equiv r_i \pmod{p}$$

sau $ai \equiv (-1)^{\alpha_i} r_i \pmod{p}$ cu $\alpha_i = 0$ și $0 < r_i < \frac{|p|}{2}$.

Dacă $\frac{|p|}{2} < R < |p|$, vom scrie

$$ai = pQ + |p| + (R - |p|)$$

sau $ai = p(Q + \operatorname{sign} p) + (R - |p|)$. Dar $\frac{|p|}{2} < R < |p|$, deci $0 < |p| - R < \frac{|p|}{2}$. Așadar, putem pune $|p| - R = r_i$ cu $0 < r_i < \frac{|p|}{2}$, deci

$$ai = p(Q + \operatorname{sign} p) - r_i,$$

deci $ai \equiv (-1)^{\alpha_i} r_i \pmod{p}$ cu $\alpha_i = 1$, $0 < r_i < \frac{|p|}{2}$.

Din cele arătate mai sus, rezultă că pentru fiecare i din $1, 2, \ldots, \frac{|p|-1}{2}$ putem determina un r_i din $1, 2, \ldots, \frac{|p|-1}{2}$ astfel încît

$$ai \equiv (-1)^{\alpha_i} r_i \pmod{p}$$

cu $\alpha_i = 0$ sau 1.

La $i \neq j$ corespunde $r_i \neq r_j$, deoarece dacă am avea $r_i = r_j$, atunci din

$$ai \equiv (-1)^{\alpha_i} r_i \pmod{p},$$
$$aj \equiv (-1)^{\alpha_j} r_j \pmod{p},$$

am obține $(-1)^{\alpha_i} ai - (-1)^{\alpha_j} aj \equiv 0 \pmod{p}$, deci $a((-1)^{\alpha_i} i - (-1)^{\alpha_j} j) \equiv 0 \pmod{p}$ și cum $p\nmid a$ și p este prim, am obține $(-1)^{\alpha_i} i - (-$

$-1)^{\alpha_j} j \equiv 0 \pmod p$. Dacă $\alpha_i = \alpha_j$ am avea $i-j \equiv 0 \pmod p$, ceea ce nu se poate decît dacă $i=j$, pentru că $|i-j| < \frac{|p|}{2}$, iar dacă $\alpha_i \neq \alpha_j$ am avea $i+j \equiv 0 \pmod p$, ceea ce iarăși nu se poate, deoarece $i+j < |p|$. Am demonstrat deci că la $i \neq j$ corespunde $r_i \neq r_j$.

Deoarece la $i \neq j$ corespunde $r_i \neq r_j$, iar r_i ia aceleași valori ca și i, înseamnă că atunci cînd i parcurge valorile $1, 2, \ldots, \frac{|p|-1}{2}$, fiecare valoare fiind parcursă o singură dată, numărul r_i parcurge, de asemenea, valorile $1, 2, \ldots, \frac{|p|-1}{2}$ fiecare valoare fiind parcursă o singură dată. Deci avem

$$a^{\frac{|p|-1}{2}} 1 \cdot 2 \cdot \ldots \cdot \frac{|p|-1}{2} \equiv (-1)^{\sum_{i=1}^{\frac{|p|-1}{2}} \alpha_i} r_1 r_2 \ldots r_{\frac{|p|-1}{2}} \pmod p$$

și $1 \cdot 2 \cdot \ldots \cdot \frac{|p|-1}{2} = r_1 r_2 \ldots r_{\frac{|p|-1}{2}}$. Deoarece $\left(1 \cdot 2 \cdot \ldots \cdot \frac{|p|-1}{2}, p\right) \cong 1$, ceea ce rezultă din aceea că numerele naturale $i \left(i = 1, \ldots, \frac{|p|-1}{2}\right)$ sînt astfel încît $i < |p|$, deci $p \nmid i$ sau $(i, p) \cong 1$, obținem

$$a^{\frac{|p|-1}{2}} \equiv (-1)^{\sum_{i=1}^{\frac{|p|-1}{2}} \alpha_i} \pmod p.$$

Dar după criteriul lui Euler avem $\left(\frac{a}{p}\right) \equiv a^{\frac{|p|-1}{2}} \pmod p$, deci $\left(\frac{a}{p}\right) \equiv (-1)^{\lambda} \pmod p$, de unde

$$\left(\frac{a}{p}\right) = (-1)^{\lambda},$$

deoarece cu p prim impar nu putem avea decît

$$1 \equiv 1 \pmod p,$$

$$-1 \equiv -1 \pmod p,$$

congruențele $1 \equiv -1 \pmod p$, $-1 \equiv 1 \pmod p$ nefiind adevărate.

11.2. Legea reciprocității pătratice

Dacă p și q sînt numere prime pozitive impare, diferite între ele, avem

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Demonstrație. Fie $p = 2k+1$, $q = 2l+1$. Dacă $\nu = 1, 2, \ldots, k$, conform criteriului lui Gauss, avem

$$\left(\frac{q}{p}\right) = (-1)^{\lambda},$$

unde $\lambda = \sum_{\nu=1}^{k} \alpha_\nu$, iar $q\nu \equiv (-1)^{\alpha_\nu} r_\nu \pmod p$, r_ν fiind un număr natural care satisface relația $r_\nu < \frac{p}{2}$.

Dacă $\alpha_\nu = 0$ atunci din $q\nu \equiv (-1)^{\alpha_\nu} r_\nu \pmod p$ se deduce $p \mid q\nu - r_\nu$, deci $q\nu - r_\nu = pS$, S fiind un număr întreg. Deci $q\nu = pS + r_\nu$, unde $0 < r_\nu < \frac{p}{2}$. Dacă $\alpha_\nu = 1$ atunci din $q\nu \equiv (-1)^{\alpha_\nu} r_\nu \pmod p$ rezultă că $p \mid q\nu - (-r_\nu)$ deci $q\nu + r_\nu = pT$, T fiind un număr întreg. Deci $q\nu = pT - r_\nu$, unde $0 < r_\nu < \frac{p}{2}$ sau $q\nu = p(T-1) + (p - r_\nu)$, unde $\frac{p}{2} < p - r_\nu < p$. În ambele cazuri ajungem la relațiile $q\nu = pQ + \rho_\nu$, $0 < \rho_\nu < p$ care exprimă aplicarea teoremei împărțirii întregi lui $q\nu$ și p și în care $\rho_\nu = r_\nu$ dacă $\alpha_\nu = 0$ și $\rho_\nu = p - r_\nu$ dacă

$\alpha_\nu=1$. Din cauză că putem scrie $\frac{q\nu}{p}=Q+\frac{\rho_\nu}{p}$, $0<\frac{\rho_\nu}{p}<1$ înseamnă că $Q=\left[\frac{q\nu}{p}\right]$. Sumînd toate egalitățile $q\nu=p\left[\frac{q\nu}{p}\right]+\rho_\nu$, $\nu=1, 2, \ldots, k$, obținem

$$q\sum_{\nu=1}^{k}\nu=p\sum_{\nu=1}^{k}\left[\frac{q\nu}{p}\right]+\sum_{\nu=1}^{k}\rho_\nu.$$

Din cauză că λ reprezintă numărul acelor ν pentru care $\alpha_\nu=1$, avem

$$\sum_{\nu=1}^{k}\rho_\nu=\sum_{\alpha_\nu=0}r_\nu+\sum_{\alpha_\nu=1}(p-r_\nu)=\sum_{\alpha_\nu=0}r_\nu-\sum_{\alpha_\nu=1}r_\nu+\lambda p,$$

suma sub care este scrisă relația $\alpha_\nu=0$, fiind extinsă la toți ν dintre $1, \ldots, k$ pentru care $\alpha_\nu=0$, iar suma sub care este scrisă relația $\alpha_\nu=1$ fiind extinsă la toți ν dintre $1, \ldots, k$ pentru care $\alpha_\nu=1$. Deci

$$q\sum_{\nu=1}^{k}\nu=p\sum_{\nu=1}^{k}\left[\frac{q\nu}{p}\right]+\sum_{\alpha_\nu=0}r_\nu-\sum_{\alpha_\nu=1}r_\nu+\lambda p.$$

Transformînd această egalitate într-o congruență modulo 2 obținem

$$\sum_{\nu=1}^{k}\nu\equiv\sum_{\nu=1}^{k}\left[\frac{q\nu}{p}\right]+\sum_{\alpha_\nu=0}r_\nu+\sum_{\alpha_\nu=1}r_\nu+\lambda \pmod 2.$$

Dar $\sum_{\alpha_\nu=0}r_\nu+\sum_{\alpha_\nu=1}r_\nu=\sum_{\nu=1}^{k}\nu$, deoarece din formularea criteriului lui Gauss rezultă că dacă ν parcurge numerele $1, \ldots, k$ fiecare număr fiind parcurs o singură dată, atunci r_ν parcurge, de asemenea, numerele $1, \ldots, k$, fiecare număr fiind parcurs o singură dată. Deci

$$\lambda\equiv\sum_{\nu=1}^{k}\left[\frac{q\nu}{p}\right]\pmod 2.$$

Notînd cu λ_1 numărul întreg care intervine în criteriul lui Gauss referitor la $\left(\frac{p}{q}\right)$ obținem

$$\lambda_1\equiv\sum_{\tau=1}^{l}\left[\frac{p\tau}{q}\right]\pmod 2.$$

Deci $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\lambda}(-1)^{\lambda_1}=(-1)^{\lambda+\lambda_1}$, unde $\lambda+\lambda_1\equiv\sum_{\nu=1}^{k}\left[\frac{q\nu}{p}\right]+\sum_{\tau=1}^{l}\left[\frac{p\tau}{q}\right]\pmod 2$, Vom arăta că

$$\sum_{\nu=1}^{k}\left[\frac{q\nu}{p}\right]+\sum_{\tau=1}^{l}\left[\frac{p\tau}{q}\right]=kl.$$

În acest scop să considerăm expresiile $q\nu-p\tau$ pentru $\nu=1, 2, \ldots, k$ și $\tau=1, 2, \ldots, l$. Avem $q\nu-p\tau\neq 0$, deoarece dacă $q\nu-p\tau=0$, atunci $p|q\nu$, deci $p|q$ sau $p|\nu$, ceea ce este contradictoriu din cauză că p și q sînt numere prime pozitive distincte, iar $0<\nu<\frac{p}{2}<p$. Deci avem $q\nu-p\tau>0$ sau $q\nu-p\tau<0$. În total avem kl expresii $q\nu-p\tau$, avînd k valori pentru ν și l valori pentru τ. Să numărăm expresiile $q\nu-p\tau$ pentru care $q\nu-p\tau>0$. Pentru fiecare ν, numărul valorilor lui τ pentru care $q\nu-p\tau>0$ este $\left[\frac{q\nu}{p}\right]$, deoarece $\tau<\frac{q\nu}{p}$ și deci τ ia valorile $1, 2, \ldots, \left[\frac{q\nu}{p}\right]$, pentru că $\tau<\frac{q\nu}{p}<\frac{q}{p}\frac{p}{2}=\frac{q}{2}$. Pentru toate valorile lui ν numărul expresiilor $q\nu-p\tau$ pentru care $q\nu-p\tau>0$ va fi deci $\sum_{\nu=1}^{k}\left[\frac{q\nu}{p}\right]$. Tot astfel $\sum_{\tau=1}^{l}\left[\frac{p\tau}{q}\right]$ reprezintă numărul expresiilor $q\nu-p\tau$ pentru care $q\nu-p\tau<0$.

Am demonstrat deci că

$$\sum_{\nu=1}^{k}\left[\frac{q\nu}{p}\right]+\sum_{\tau=1}^{l}\left[\frac{p\tau}{q}\right]=kl.$$

Deci $\lambda+\lambda_1\equiv kl \pmod 2$, deci

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{kl}=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

11.3. Calculul simbolurilor lui Legendre $\left(\frac{-1}{p}\right),\left(\frac{2}{p}\right),\left(\frac{-3}{p}\right)$

(1) $\left(\frac{-1}{p}\right)=(-1)^{\frac{|p|-1}{2}}$ *sau* $\left(\frac{-1}{p}\right)=\begin{cases}1 & \text{dacă } |p|\equiv 1 \pmod 4,\\ -1 & \text{dacă } |p|\equiv -1 \pmod 4.\end{cases}$

Demonstrație. Valoarea lui $\left(\frac{-1}{p}\right)$ rezultă din criteriul lui Euler deoarece, după acest criteriu,

$$\left(\frac{-1}{p}\right)\equiv(-1)^{\frac{|p|-1}{2}} \pmod p.$$

Din cauză că nu putem avea $1\equiv -1 \pmod p$, $-1\equiv 1 \pmod p$, ci putem avea numai $1\equiv 1 \pmod p$, $-1\equiv -1 \pmod p$, p fiind prim impar, atunci

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{|p|-1}{2}} \text{ sau } \left(\frac{-1}{p}\right)=\begin{cases}1 \text{ dacă } |p|\equiv 1 \pmod 4,\\ -1 \text{ dacă } |p|\equiv -1 \pmod 4.\end{cases}$$

(2) $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}=(-1)^{\frac{p^*-1}{4}}$, *unde* $p^*\equiv 1 \pmod 4$ *și* $p^*=(-1)^{\alpha}p$, α *fiind un număr întreg.*

Demonstrație. Vom aplica criteriul lui Gauss. Punînd $|p|=2k+1$ se constată că

$$2\nu\equiv(-1)^{\alpha_\nu}r_\nu \pmod p,$$

unde $r_\nu=2\nu$, $\alpha_\nu=0$ dacă $0<2\nu<\frac{|p|}{2}$ și

$$2\nu\equiv(-1)^{\alpha_\nu}r_\nu \pmod p,$$

unde $r_\nu=|p|-2\nu$, $\alpha_\nu=1$ dacă $\frac{|p|}{2}<2\nu<|p|$, deoarece cu $\nu=1,2,\ldots,k$ nu putem avea decît $0<2\nu<|p|$. Deci $\lambda=\sum_{\nu=1}^{\frac{|p|-1}{2}}\alpha_\nu$ este egal cu numărul acelor ν pentru care $\frac{|p|}{2}<2\nu<|p|$. Ținînd seama de faptul că aceste inegalități le putem scrie $|p|<4\nu$, $2\nu<|p|$ și avînd în vedere că ultimele inegalități sînt între numere întregi, deducem $|p|+1\leqslant 4\nu$, $2\nu\leqslant|p|-1$, deci

$$\frac{|p|+1}{4}\leqslant\nu\leqslant\frac{|p|-1}{2}.$$

Numărul p este impar și deci $\frac{|p|-1}{2}$ este un număr întreg. Dacă $\frac{|p|+1}{4}$ este un număr întreg, ceea ce este echivalent cu $|p|\equiv -1 \pmod 4$, rezultă că numărul numerelor întregi ν care verifică inegalitățile

$$\frac{|p|+1}{4}\leqslant\nu\leqslant\frac{|p|-1}{2}$$

este

$$\lambda=\frac{|p|-1}{2}-\left(\frac{|p|+1}{4}-1\right)=\frac{|p|+1}{4}.$$

Dacă $\frac{|p|+1}{4}$ nu este număr întreg, atunci $|p|\not\equiv -1 \pmod 4$. Deci $|p|\equiv 1 \pmod 4$, pentru că $|p|$ este impar. Dar atunci $|p|+3\equiv 4 \pmod 4$ deci $4\mid|p|+3$ deci $\frac{|p|+3}{4}$ este număr întreg. Avînd $\frac{|p|+3}{4}$ —

$-\frac{|p|+1}{4}=\frac{1}{2}<1$ înseamnă că cel mai mic număr întreg care este mai mare decît $\frac{|p|+1}{4}$ este $\frac{|p|+3}{4}$, deci în acest caz

$$\frac{|p|+3}{4}\leqslant \nu \leqslant \frac{|p|-1}{2}.$$

Numărul numerelor întregi ν care verifică inegalitățile de mai sus este

$$\lambda=\frac{|p|-1}{2}-\left(\frac{|p|+3}{4}-1\right)=\frac{|p|-1}{4}.$$

Deci

$$\left(\frac{2}{p}\right)=\begin{cases}(-1)^{\frac{|p|+1}{4}} \text{ dacă } |p|\equiv -1 \pmod 4,\\ (-1)^{\frac{|p|-1}{4}} \text{ dacă } |p|\equiv 1 \pmod 4.\end{cases}$$

Se constată acum că din $|p|\equiv -1 \pmod 4$ rezultă $|p|=-1+4t$, unde t este un număr întreg, deci

$$p^2=|p|^2=1-8t+16t^2=1-8(t-2t^2),$$

de unde

$$\frac{p^2-1}{8}=-t+2t^2=\frac{|p|+1}{4}-2t+2t^2.$$

De asemenea cu $p^*\equiv 1 \pmod 4$, $p^*=(-1)^{\alpha}p$ și $|p|\equiv -1 \pmod 4$ rezultă $p^*=-|p|$, deoarece $p^*=|p|$ cu $p^*\equiv 1 \pmod 4$ contrazice pe $|p|\equiv -1 \pmod 4$. Deci

$$p^*=1-4t,$$

deci

$$\frac{p^*-1}{4}=-t=\frac{|p|+1}{4}-2t.$$

Am ajuns la concluzia că în cazul cînd $|p|\equiv -1 \pmod 4$, avem

$$(-1)^{\frac{|p|+1}{4}}=(-1)^{\frac{p^2-1}{8}}=(-1)^{\frac{p^*-1}{4}}.$$

Dacă $|p|\equiv 1 \pmod 4$ obținem $|p|=1+4s$, unde s este un număr întreg, deci

$$p^2=|p|^2=1+8s+16s^2=1+8(s+2s^2),$$

de unde

$$\frac{p^2-1}{8}=s+2s^2=\frac{|p|-1}{4}+2s^2.$$

De asemenea cu $p^*\equiv 1 \pmod 4$, $p^*=(-1)^{\alpha}p$ și $|p|\equiv 1 \pmod 4$ rezultă $p^*=|p|$, deoarece $p^*=-|p|$ cu $p^*\equiv 1 \pmod 4$ contrazice pe $|p|\equiv 1 \pmod 4$. Deci

$$p^*=1+4s,$$

deci

$$\frac{p^*-1}{4}=s=\frac{|p|-1}{4}.$$

Am ajuns la concluzia că și în cazul cînd $|p|\equiv 1 \pmod 4$, avem

$$(-1)^{\frac{|p|-1}{4}}=(-1)^{\frac{p^2-1}{8}}=(-1)^{\frac{p^*-1}{4}},$$

deci proprietatea (2) este demonstrată.

(3) $\left(\frac{-3}{p}\right)=\begin{cases}1 \text{ } \textit{dacă } p\equiv 1 \pmod 6,\\ -1 \text{ } \textit{dacă } p\equiv -1 \pmod 6,\end{cases}$

unde p este un număr prim pozitiv impar diferit de 3.

Demonstrație. Utilizînd proprietățile, stabilite pînă acum, ale simbolului lui Legendre, avem

$$\left(\frac{-3}{p}\right)=\left(\frac{-1\cdot 3}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)=(-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}\frac{3-1}{2}}=\left(\frac{p}{3}\right)=\left(\frac{r}{3}\right)$$

cu $p\equiv r \pmod 3$, $r=0, 1, 2$. Nu putem avea $r=0$, deoarece dacă $r=0$ avem $3|p$, ceea ce nu este posibil, p fiind prim pozitiv diferit de 3. Dacă $r=1$ atunci $\left(\frac{1}{3}\right)=1$. Dacă $r=2$ atunci $\left(\frac{2}{3}\right)=(-1)^{\frac{-3-1}{4}}=$

$=-1$. Dar $p\equiv 2 \pmod 3$ este echivalent cu $p\equiv -1 \pmod 3$. De asemenea, $3|p\pm 1$ este echivalent cu $6|p\pm 1$, deoarece p este impar, deci proprietatea de mai sus este demonstrată.

Aplicație. Vrem să știm dacă congruența

$$x^2\equiv 10 \pmod{13}$$

are sau nu soluții.

Dacă ne-am referi la teoria generală a resturilor de grad n ar trebui să cunoaștem o rădăcină primitivă modulo 13. Utilizînd simbolul lui Legendre putem evita căutarea rădăcinilor primitive modulo 13 făcînd următorul calcul

$$\left(\frac{10}{13}\right)=\left(\frac{2\cdot 5}{13}\right)=\left(\frac{2}{13}\right)\left(\frac{5}{13}\right)=(-1)^{\frac{13-1}{4}}(-1)^{\frac{5-1}{2}\cdot\frac{13-1}{2}}\left(\frac{13}{5}\right)=-\left(\frac{13}{5}\right)=$$

$$=-\left(\frac{3}{5}\right)=-(-1)^{\frac{5-1}{2}\cdot\frac{3-1}{2}}\left(\frac{5}{3}\right)=-\left(\frac{5}{3}\right)=-\left(\frac{2}{3}\right)=-(-1)^{\frac{-3-1}{4}}=1,$$

deci 10 este rest pătratic modulo 13 și în consecință $x^2\equiv 10 \pmod{13}$ are soluții.

11.4. Simbolul lui Jacobi

Necesitatea de a descompune numărul întreg a din simbolul lui Legendre $\left(\frac{a}{p}\right)$ în factori primi, pentru a calcula acest simbol, îngreuiază acest calcul. Această dificultate este învinsă de simbolul lui Jacobi care se definește astfel:

Definiție. *Simbolul lui Jacobi este o funcție numerică, care se notează cu* $\left(\frac{a}{m}\right)$, *definită prin*

$$\left(\frac{a}{m}\right)=\prod_{i=1}^{r}\left(\frac{a}{p_i}\right)^{\alpha_i},$$

unde a și m sînt numere întregi, m fiind impar, $m=\pm p_1^{\alpha_1}p_2^{\alpha_2}\dots p_r^{\alpha_r}$, $p_1, p_2, \dots, p_r$ fiind numere prime impare neasociate două cîte două, iar $\alpha_1, \alpha_2, \dots, \alpha_r$ numere naturale.

Teoremă. *Simbolul lui Jacobi* $\left(\frac{a}{m}\right)$ *este caracter modulo* m.

Demonstrație.

$(A)\left(\frac{a}{m}\right)=0$ dacă $(a, m)\not\equiv 1$, deoarece există în acest caz un număr prim p care divide și pe a și pe m, deci în produsul care definește pe $\left(\frac{a}{m}\right)$ avem ca factor pe $\left(\frac{a}{p}\right)=0$.

$(B)\left(\frac{1}{m}\right)\neq 0$ din cauză că dacă $m\neq\pm 1$ pentru orice factor prim p al lui m avem $\left(\frac{1}{p}\right)=1$ și deci $\left(\frac{1}{m}\right)=1\neq 0$, iar dacă $m=\pm 1$, atunci în produsul care definește pe $\left(\frac{1}{m}\right)$ nu figurează nici un factor și deci acest produs este egal cu 1.

$(C)\left(\frac{ab}{m}\right)=\left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$, deoarece $\left(\frac{ab}{m}\right)=\prod_{i=1}^{r}\left(\frac{ab}{p_i}\right)^{\alpha_i}=$

$$=\prod_{i=1}^{r}\left(\frac{a}{p_i}\right)^{\alpha i}\prod_{i=1}^{r}\left(\frac{b}{p_i}\right)^{\alpha_i}=\left(\frac{a}{m}\right)\left(\frac{b}{m}\right).$$

$(D)\left(\frac{a}{m}\right)=\left(\frac{b}{m}\right)$ dacă $a\equiv b \pmod m$. În adevăr, din $a\equiv b \pmod m$ dacă $m\neq\pm 1$ rezultă $a\equiv b \pmod p$, oricare ar fi numărul prim p al lui m. Dar atunci $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$ și deci $\left(\frac{a}{m}\right)=\prod_{i=1}^{r}\left(\frac{a}{p_i}\right)^{\alpha_i}=\prod_{i=1}^{r}\left(\frac{b}{p_i}\right)^{\alpha_i}=$

$=\left(\frac{b}{m}\right)$. Dacă $m=\pm 1$ atunci, conform raționamentului din demonstrația proprietății (B), avem $\left(\frac{a}{m}\right)=1$, $\left(\frac{b}{m}\right)=1$ și deci $\left(\frac{a}{m}\right)=\left(\frac{b}{m}\right)$.

Legea reciprocității pătratice formulată cu ajutorul simbolului lui Jacobi arată în felul următor :

Dacă P și Q sînt numere întregi impare pozitive prime între ele atunci

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right)=(-1)^{\frac{P-1}{2}\frac{Q-1}{2}}.$$

Demonstrație. Dacă cel puțin unul dintre P și Q este egal cu 1 atunci atît $\left(\frac{P}{Q}\right)=1$ cît și $\left(\frac{Q}{P}\right)=1$, iar $(-1)^{\frac{P-1}{2}\frac{Q-1}{2}}=1$ și deci proprietatea este adevărată.

Dacă $P\neq 1$ și $Q\neq 1$ atunci $P=p_1^{\alpha_1}\dots p_r^{\alpha_r}$, $Q=q_1^{\beta_1}\dots q_s^{\beta_s}$, $p_1, \dots, p_r$, $q_1, \dots, q_s$ fiind numere prime pozitive diferite două cîte două, deoarece $(P, Q)\cong 1$, $\alpha_1, \dots, \alpha_r$, $\beta_1. \dots, \beta_s$ fiind numere naturale. Deci

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right)=\prod_{j=1}^{s}\left(\frac{P}{q_j}\right)^{\beta_j}\prod_{i=1}^{r}\left(\frac{Q}{p_i}\right)^{\alpha_i}=$$

$$=\prod_{j=1}^{s}\prod_{i=1}^{r}\left(\frac{p_i}{q_j}\right)^{\alpha_i\beta_j}\prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{q_j}{p_i}\right)^{\alpha_i\beta_j}=$$

$$=\prod_{i=1}^{r}\prod_{j=1}^{s}\left(\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right)\right)^{\alpha_i\beta_j}=\prod_{i=1}^{r}\prod_{j=1}^{s}(-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}\alpha_i\beta_j}=$$

$$=(-1)^{\sum_{i=1}^{r}\sum_{j=1}^{s}\frac{p_i-1}{2}\frac{q_j-1}{2}\alpha_i\beta_j}=(-1)^{\left(\sum_{i=1}^{r}\frac{p_i-1}{2}\alpha_i\right)\left(\sum_{j=1}^{s}\frac{q_j-1}{2}\beta_j\right)}.$$

Dar din $P=p_1^{\alpha_1}\dots p_r^{\alpha_r}$ deducem $P=\left(2\frac{p_1-1}{2}+1\right)^{\alpha_1}\dots\left(2\frac{p_r-1}{2}+1\right)^{\alpha_r}=1+2\sum_{i=1}^{r}\frac{p_i-1}{2}\alpha_i+4N$, unde N este un număr întreg.

Deci

$$\frac{P-1}{2}=\sum_{i=1}^{r}\frac{p_i-1}{2}\alpha_i+2N.$$

Tot astfel obținem

$$\frac{Q-1}{2}=\sum_{j=1}^{s}\frac{q_j-1}{2}\beta_j+2N_1$$

și deci

$$(-1)^{\left(\sum_{i=1}^{r}\frac{p_i-1}{2}\alpha_i\right)\left(\sum_{j=1}^{s}\frac{q_j-1}{2}\beta_j\right)}=(-1)^{\frac{P-1}{2}\frac{Q-1}{2}}.$$

Calculul simbolurilor lui Jacobi $\left(\frac{-1}{m}\right)$, $\left(\frac{2}{m}\right)$.

(1) $\left(\frac{-1}{m}\right)=(-1)^{\frac{|m|-1}{2}}$ *sau* $\left(\frac{-1}{m}\right)=\begin{cases}1 & \text{dacă } |m|\equiv 1 \pmod 4,\\ -1 & \text{dacă } |m|\equiv -1 \pmod 4.\end{cases}$

Demonstrație. Dacă $m=\pm 1$ proprietatea este demonstrată, deoarece în acest caz $\left(\frac{-1}{m}\right)=1$ și $|m|=1$, $|m|\equiv 1 \pmod 4$. Dacă $m\neq\pm 1$ avem $|m|=p_1^{\alpha_1}\dots p_r^{\alpha_r}$. Dar

$$\left(\frac{-1}{m}\right)=\prod_{i=1}^{r}\left(\frac{-1}{p_i}\right)^{\alpha_i}=\prod_{i=1}^{r}(-1)^{\frac{p_i-1}{2}\alpha_i}=(-1)^{\sum_{i=1}^{r}\frac{p_i-1}{2}\alpha_i}=(-1)^{\frac{|m|-1}{2}}$$

avînd în vedere că

$$\frac{|m|-1}{2}=\sum_{i=1}^{r}\frac{p_i-1}{2}\alpha_i+2N,$$

unde N este un număr întreg, conform celor spuse în cadrul demonstrației legii reciprocității pătratice formulate cu ajutorul simbolului lui Jacobi.

(2) $\left(\frac{2}{m}\right)=(-1)^{\frac{m^2-1}{8}}=(-1)^{\frac{m^*-1}{4}}$, *unde* $m^*\equiv 1 \pmod 4$ *și* $m^*=(-1)^{\alpha} m$, α *fiind un număr întreg.*

Demonstrație. Dacă $m=\pm 1$ proprietatea este evidentă.

Dacă $m\neq\pm 1$ avem $m=\pm p_1^{\alpha_1}\dots p_r^{\alpha_r}$, unde $p_1, \dots, p_r$ sînt numere prime pozitive impare diferite două cîte două, iar $\alpha_1, \dots, \alpha_r$ sînt numere naturale. Deoarece

$$\left(\frac{2}{m}\right)=\prod_{i=1}^{r}\left(\frac{2}{p_i}\right)^{\alpha_i}=\prod_{i=1}^{r}(-1)^{\frac{p_i^2-1}{8}\alpha_i}=(-1)^{\sum_{i=1}^{r}\frac{p_i^2-1}{8}\alpha_i}$$

și datorită faptului că

$$m^2=(p_1^2)^{\alpha_1}\dots(p_r^2)^{\alpha_r}=\left(8\frac{p_1^2-1}{8}+1\right)^{\alpha_1}\dots\left(8\frac{p_r^2-1}{8}+1\right)^{\alpha_r}=$$

$$=1+8\sum_{i=1}^{r}\frac{p_i^2-1}{8}\alpha_i+64N,$$

N fiind un număr întreg, avem

$$\frac{m^2-1}{8}=\sum_{i=1}^{r}\frac{p_i^2-1}{8}\alpha_i+8N$$

și obținem

$$\left(\frac{2}{m}\right)=(-1)^{\frac{m^2-1}{8}}.$$

Numărul întreg m fiind impar putem avea $m\equiv 1 \pmod 4$ sau $m\equiv 3 \pmod 4$. Dacă $m\equiv 1 \pmod 4$ atunci $m^*=m$, deoarece $m^*=-m$ și $m^*\equiv 1 \pmod 4$ contrazic pe $m\equiv 1 \pmod 4$. Ținînd seama de $\left(\frac{2}{m}\right)=(-1)^{\frac{m^2-1}{8}}$ obținem $\left(\frac{2}{m}\right)=(-1)^{\frac{m-1}{4}\frac{m+1}{2}}=\left((-1)^{\frac{m+1}{2}}\right)^{\frac{m-1}{4}}$,

Dar $m+1\equiv 2 \pmod 4$ sau $\frac{m+1}{2}\equiv 1 \pmod 2$ deci $(-1)^{\frac{m+1}{2}}=-1$ și deci

$$\left(\frac{2}{m}\right)=(-1)^{\frac{m^*-1}{4}}.$$

Dacă $m\equiv 3 \pmod 4$ atunci $m^*=-m$, deoarece $m^*=m$ și $m^*\equiv 1 \pmod 4$ contrazic pe $m\equiv 3 \pmod 4$. Ținînd seama de $\left(\frac{2}{m}\right)=(-1)^{\frac{m^2-1}{8}}$ obținem $\left(\frac{2}{m}\right)=(-1)^{\frac{m-1}{2}\frac{m+1}{4}}=\left((-1)^{\frac{m-1}{2}}\right)^{\frac{m-1}{4}}$. Dar $m-1\equiv 2 \pmod 4$ sau $\frac{m-1}{2}\equiv 1 \pmod 2$ deci $(-1)^{\frac{m-1}{2}}=-1$ și deci $\left(\frac{2}{m}\right)=(-1)^{\frac{m^*-1}{4}}$.

Aplicație. Pentru a vedea dacă congruența

$$x^2\equiv 21 \pmod{23}$$

are sau nu soluții, vom calcula simbolul lui Legendre $\left(\frac{21}{23}\right)$ considerîndu-l drept simbolul lui Jacobi. Atunci

$$\left(\frac{21}{23}\right)=(-1)^{\frac{21-1}{2}\frac{23-1}{2}}\left(\frac{23}{21}\right)=(-1)^{\frac{20}{2}\frac{22}{2}}\left(\frac{2}{21}\right)=(-1)^{\frac{21-1}{4}}=-1.$$

Deci congruența considerată nu are soluții.

Capitolul 12

INFINITATEA NUMERELOR PRIME

12.1. Teorema lui Euclid

Un număr prim este un număr întreg diferit de 0 și de ± 1 care are proprietatea că oricare ar fi produsul ab de numere întregi astfel încît $p|ab$ rezultă că $p|a$ sau $p|b$.

Teorema lui Euclid afirmă că :

Teoremă. *Există o infinitate de numere prime.*

Una din demonstrațiile date acestei teoreme este următoarea.

Presupunem că există numai un număr finit de numere prime pozitive. În acest caz, numerele prime pozitive care există le notăm cu $p_1, \ldots, p_n$ și alcătuim un număr natural N astfel încît $N = p_1 \ldots p_n + 1$. Dacă nu există nici un număr prim pozitiv, considerăm că produsul $p_1 \ldots p_n$ este înlocuit cu 1. Deci $N > 1$ și prin urmare există un factor prim pozitiv p al lui N. Trebuie ca p să fie diferit de $p_1, \ldots, p_n$, deoarece dacă p este unul din $p_1, \ldots, p_n$ avem $p|p_1 \ldots p_n$ și cum $p|N$ rezultă $p|N - p_1 \ldots p_n$ deci $p|1$ ceea ce nu se poate, deoarece $p \neq \pm 1$. Dar existența unui număr prim p diferit de $p_1, \ldots, p_n$ contrazice presupunerea făcută. Deci teorema lui Euclid este demonstrată avînd în vedere că dacă există o infinitate de numere prime pozitive, există și o infinitate de numere prime.

O altă demonstrație a teoremei lui Euclid este următoarea.

Se presupune că există numai un număr finit de numere prime pozitive. Datorită acestei presupuneri putem să numerotăm numerele prime care există în felul următor : $p_1, \ldots, p_n$. Se constată că

$$\prod_{i=1}^{n} \frac{1}{1-\frac{1}{p_i}} = \prod_{i=1}^{n} \sum_{k=0}^{\infty} \frac{1}{p^k} = \sum_{n=1}^{\infty} \frac{1}{n}.$$

Avem dreptul să dezvoltăm în serie pe $\dfrac{1}{1-\frac{1}{p_i}}$, deoarece $\left|\dfrac{1}{p_i}\right| < 1$.

Fiecare din seriile obținute este absolut convergentă și de aceea avem dreptul să facem produsul lor. Produsul obținut este seria armonică, deoarece produsul $p_1^{\alpha_1} \ldots p_n^{\alpha_n}$, unde $\alpha_1, \ldots, \alpha_n$ sînt numere întregi nenegative, este un număr natural. Fiecare număr natural este obținut o singură dată datorită teoremei unicității descompunerii numerelor întregi în factori primi. Datorită teoremei de existență a descompunerii numerelor întregi în factori primi, orice număr natural poate fi scris sub forma $p_1^{\alpha_1} \ldots p_n^{\alpha_n}$, unde $\alpha_1 \ldots, \alpha_n$ sînt numere întregi nenegative, deoarece, conform presupunerii făcute, $p_1, \ldots, p_n$ sînt singurele numere prime pozitive care există. Dar seria armonică este divergentă, pe cînd produsul

$$\prod_{i=1}^{n} \frac{1}{1-\frac{1}{p_i}}$$

este finit, datorită presupunerii că există numai un număr finit de numere prime pozitive. Contradicția la care am ajuns demonstrează teorema lui Euclid.

Se spune că prima demonstrație este dată cu metoda lui Euclid.

12.2. Teorema lui Dirichlet

O generalizare a teoremei lui Euclid constă în teorema lui Dirichlet.

Teoremă. *În orice clasă de resturi primă cu modulul există o infinitate de numere prime.*

Aceeași teoremă poate fi enunțată și în felul următor.

Teoremă. *În orice progresie aritmetică $a+km$ în care rația m este primă cu primul termen a, există o infinitate de numere prime pozitive.*

Noul enunț este echivalent cu primul, deoarece două numere $a+k_1m$, $a+k_2m$ dintr-o aceeași progresie aritmetică fac parte din aceeași clasă de resturi modulo m avînd $(a+k_1m)-(a+k_2m)=(k_1-k_2)m$, adică avînd $m|(a+k_1m)-(a+k_2m)$ și deoarece, reciproc, numerele dintr-o clasă de resturi modulo m formează o progresie aritmetică cu rația egală cu m, primul termen fiind un număr din clasa de resturi considerată, avînd $m|b-a$, adică $b=a+km$, a și b fiind două numere oarecare din clasa de resturi considerată.

Nu vom demonstra, în acest capitol, teorema lui Dirichlet, deoarece nu este cunoscută nici o demonstrație a acestei teoreme efectuată cu mijloace elementare. Vom demonstra însă această teoremă în cîteva cazuri particulare, iar metoda pe care o vom folosi va fi metoda lui Euclid expusă mai sus.

12.3. Demonstrația teoremei lui Dirichlet în cazul progresiilor aritmetice $-1+k4$ și $-1+k6$

Teoremă. *În progresia aritmetică $-1+k4$ există o infinitate de numere prime pozitive.*

Demonstrație. Presupunem că există numai un număr finit de numere prime pozitive de forma $-1+k4$ și apoi pe toate care există le notăm cu $p_1 \ldots, p_n$. Numărul ajutător $-1+p_1 \ldots p_n 4$ pe care-l notăm cu N este mai mare ca 1, avînd $p_1 \ldots p_n \neq 0$, aceasta și în cazul cînd nu există nici un număr prim pozitiv de forma $-1+k4$, deoarece în acest caz se consideră că $p_1 \ldots p_n = 1$. Numărul N admite deci cel puțin un factor prim pozitiv. Dar acest lucru nu este suficient. Trebuie să arătăm că numărul N admite cel puțin un factor prim pozitiv de forma $-1+k4$. În acest fapt constă

toată dificultatea demonstrării cazurilor particulare ale teoremei lui Dirichlet, atunci cînd utilizăm metoda lui Euclid.

Să vedem, în acest scop, de ce formă pot fi numerele prime pozitive atunci cînd le împărțim cu 4. Dacă p este un număr prim pozitiv, prin aplicarea teoremei împărțirii întregi lui p pozitiv și 4 obținem

$$p=4q+r, \quad 0 \leqslant r<4.$$

Nu putem avea $r=0$, deoarece dacă $r=0$ avem $p=4q$ și deci p nu este prim, deoarece dacă ar fi prim, din $p=4q$ ar rezulta $p|2$, deci $p \leqslant 2$, ceea ce este contradictoriu.

Din $r=1$ nu rezultă nici o contradicție din faptul că p este prim și $p=4q+1$, deci putem avea numere prime pozitive de forma $1+k4$, unde am pus $k=q$.

Nu putem avea $r=2$ decît dacă $p=2$, deoarece dacă $r=2$ avem $p=4q+2=2(2q+1)$. Dacă p este prim trebuie ca $p|2$ deci $p \leqslant 2$ sau $p=2$, deoarece $p \neq 1$. Putem avea $p=2$ luînd $q=0$.

Din $r=3$ nu rezultă nici o contradicție din faptul că p este prim și $p=4q+3$, deci putem avea numere prime pozitive de forma $-1+k4$, unde am pus $k=q+1$.

Am demonstrat deci că orice număr prim pozitiv diferit de 2 este de forma $1+k4$ sau de forma $-1+k4$, cuvîntul „sau" avînd sens de excludere, din cauza unicității cîtului și restului în teorema împărțirii întregi.

Să demonstrăm, acum, că numărul N de mai sus admite cel puțin un divizor prim pozitiv de forma $-1+k4$. Să presupunem prin absurd că N admite numai divizori primi pozitivi de forma $1+k4$. Prin înmulțirea acestor divizori primi pozitivi obținem că N este de forma $1+k4$, ceea ce contrazice faptul că N este de forma $-1+k4$, ceea ce rezultă din felul cum a fost alcătuit N. Contrazicerea rezultă din aceea că în teorema împărțirii întregi cîtul și restul sînt unice, cele două forme ale lui N, una obținută prin înmulțirea divizorilor săi primi pozitivi de forma $1+k4$ și alta obținută din $-1+p_1 \ldots p_n 4=4(p_1 \ldots p_n-1)+3$ putînd fi interpretate ca fiind obținute prin aplicarea teoremei împărțirii întregi lui N și 4. Din această contrazicere rezultă că N admite cel puțin un divizor prim p pozitiv de forma $-1+k4$. Dar atunci

$$p|N, \quad p|p_1 \ldots p_n,$$

deoarece $p_1, \ldots, p_n$ sînt toate numerele prime pozitive de forma $-1+k4$, deci $p|N-4p_1 \ldots p_n$, deci $p|-1$, ceea ce este contradic-

toriu, deoarece numerele prime nu sînt unități. Teorema enunțată a fost deci demonstrată.

Teoremă. *În progresia aritmetică* $-1+k6$ *există o infinitate de numere prime pozitive.*

Demonstrație. Presupunem că există numai un număr finit de numere prime pozitive de forma $-1+k6$ și pe toate care există le notăm cu $p_1, \ldots, p_n$. Numărul ajutător $-1+p_1 \ldots p_n 6$ pe care-l notăm cu N este mai mare ca 1, avînd $p_1 \ldots p_n \neq 0$, aceasta și în cazul cînd nu există nici un număr prim pozitiv de forma $-1+k6$, deoarece în acest caz se consideră că $p_1 \ldots p_n = 1$.

Pentru a arăta că N admite cel puțin un divizor prim pozitiv de forma $-1+k6$, trebuie să vedem, mai întîi, de ce formă pot fi numerele prime pozitive atunci cînd le dividem la 6.

Aplicînd teorema împărțirii întregi unui număr prim pozitiv p și lui 6 obținem

$$p = 6q + r, \quad 0 \leqslant r < 6.$$

Nu putem avea $r=0$, deoarece dacă $r=0$, numărul $p=6q$ nu este prim, deoarece dacă ar fi prim, din $p=6q$ ar rezulta că $p|2$, deci $p \leqslant 2$, ceea ce este contradictoriu.

Cu $r=1$ nu rezultă nici o contradicție din faptul că p este prim și $p=6q+1$, deci putem avea numere prime pozitive de forma $1+k6$, unde am pus $k=q$.

Nu putem avea $r=2$ decît dacă $p=2$. Într-adevăr, dacă $r=2$, atunci $p=6q+2=2(3q+1)$. Dacă p este prim, trebuie ca $p|2$ deci $p \leqslant 2$ sau $p=2$, deoarece $p \neq 1$. Putem avea $p=2$ luînd $q=0$.

Nu putem avea $r=3$ decît dacă $p=3$. Într-adevăr, dacă $r=3$, atunci $p=6q+3=3(2q+1)$. Dacă p este prim, trebuie ca $p|3$ deci $p \leqslant 3$ sau $p=3$, deoarece $p \neq 1$ și este impar. Putem avea $p=3$ luînd $q=0$.

Nu putem avea $r=4$. Într-adevăr, dacă $r=4$, atunci $p=6q+4=2(3q+2)$. Dacă p este prim trebuie ca $p|2$ deci $p \leqslant 2$ sau $p=2$, deoarece $p \neq 1$. Nu putem însă avea $p=2$, deoarece dacă $p=2$ avem $2=2(3q+2)$ sau $3q=-1$, ceea ce în numere întregi este contradictoriu.

Cu $r=5$ nu rezultă nici o contradicție din faptul că p este prim și $p=6q+5$, deci putem avea numere prime pozitive de forma $-1+k6$, unde am pus $k=q+1$.

Să demonstrăm, acum, că numărul N de mai sus admite cel puțin un divizor prim pozitiv de forma $-1+k6$. Să presupunem

prin absurd că N admite numai divizori primi pozitivi de forma $1+k6$. Prin înmulțirea acestor divizori primi pozitivi obținem că N este de forma $1+k6$, ceea ce contrazice faptul că N este de forma $-1+k6$, ceea ce rezultă din felul cum a fost alcătuit N. Contrazicerea rezultă din aceea că în teorema împărțirii întregi cîtul și restul sînt unice, cele două forme ale lui N, una obținută prin înmulțirea divizorilor săi primi pozitivi de forma $1+k6$ și alta obținută din $-1+p_1 \ldots p_n 6 = 6(p_1 \ldots p_n - 1)+5$ putînd fi interpretate ca fiind obținute prin aplicarea teoremei împărțirii întregi lui N și 6. Din această contrazicere rezultă că N admite cel puțin un divizor prim p pozitiv de forma $-1+k6$. Dar atunci

$$p|N, \quad p|p_1 \ldots p_n,$$

deoarece $p_1, \ldots, p_n$ sînt toate numerele prime pozitive de forma $-1+k6$, deci $p|N-6p_1 \ldots p_n$, deci $p|-1$, ceea ce este contradictoriu, deoarece numerele prime nu sînt unități. Teorema enunțată a fost deci demonstrată.

12.4. Demonstrația teoremei lui Dirichlet în cazul progresiilor aritmetice $1+k4$ și $1+k6$ cu ajutorul resturilor pătratice

Teoremă. *În progresia aritmetică* $1+k4$ *există o infinitate de numere prime pozitive.*

Demonstrație. Presupunem că există numai un număr finit de numere prime pozitive de forma $1+k4$ și pe toate care există le notăm cu $p_1, \ldots, p_n$. Numărul ajutător $1+(2p_1 \ldots p_n)^2$, pe care-l notăm cu N este mai mare ca 1, avînd $p_1 \ldots p_n \neq 0$, aceasta și în cazul cînd nu există nici un număr prim pozitiv de forma $1+k4$, deoarece în acest caz se consideră că $p_1 \ldots p_n = 1$.

Divizorii primi pozitivi ai lui N sînt impari, deoarece din felul cum este alcătuit N rezultă că $2 \nmid N$. Fie p un divizor prim pozitiv impar al lui N. Un astfel de divizor există, deoarece $N > 1$ și $2 \nmid N$.

Obținem

$$p|1+(2p_1 \ldots p_n)^2$$

sau

$$(2p_1 \ldots p_n)^2 \equiv -1 \pmod{p},$$

deci simbolul lui Legendre $\left(\frac{-1}{p}\right)$ este egal cu 1, deoarece -1 este rest pătratic modulo p. Dar acest lucru înseamnă că p este de forma $1+k4$.

Am dovedit că N admite cel puțin un divizor prim pozitiv de forma $1+k4$. Asta înseamnă că

$$p|N,\ p|p_1 \ldots p_n,$$

deoarece $p_1, \ldots, p_n$ sînt toate numerele prime pozitive de forma $1+k4$, deci $p|N-(2p_1 \ldots p_n)^2$, deci $p|1$, ceea ce este contradictoriu, deoarece numerele prime nu sînt unități. Teorema enunțată a fost deci demonstrată.

Teoremă. *În progresia aritmetică* $1+k6$ *există o infinitate de numere prime pozitive.*

Demonstrație. Presupunem că există numai un număr finit de numere prime pozitive de forma $1+k6$ și toate care există le notăm cu $p_1, \ldots, p_n$. Numărul ajutător $3+(2p_1 \ldots p_n)^2$ pe care-l notăm cu N este mai mare ca 1, avînd $N>3$.

Divizorii primi pozitivi ai lui N sînt impari, deoarece din felul cum este alcătuit N rezultă că $2 \nmid N$. Fie p un divizor prim pozitiv impar al lui N. Un astfel de divizor există, deoarece $N>1$ și $2 \nmid N$.

Obținem

$$p|3+(2p_1 \ldots p_n)^2$$

sau

$$(2p_1 \ldots p_n)^2 \equiv -3 \pmod{p},$$

deci simbolul lui Legendre $\left(\frac{-3}{p}\right)$ este egal cu 1, deoarece -3 este rest pătratic modulo p. Dar acest lucru înseamnă că p este de forma $1+k6$.

Am dovedit că N admite cel puțin un divizor prim pozitiv de forma $1+k6$. Aceasta înseamnă că

$$p|N,\ p|p_1 \ldots p_n,$$

deoarece $p_1, \ldots, p_n$ sînt toate numerele prime pozitive de forma $1+k6$, deci $p|N-(2p_1 \ldots p_n)^2$, deci $p|3$, deci $p=3$, p fiind prim și pozitiv, ceea ce este contradictoriu, deoarece 3 prin împărțire la 6 nu dă rest 1, cum dă p prin împărțire la 6. Teorema enunțată a fost deci demonstrată.

12.5. Demonstrația teoremei lui Dirichlet în cazul progresiilor aritmetice $1+4k$ și $1+k6$ fără ajutorul resturilor pătratice

Teoremă. *În progresia aritmetică* $1+k4$ *există o infinitate de numere prime pozitive.*

Demonstrație. Vom păstra demonstrația dată acestei teoreme mai sus cu singura deosebire că vom demonstra existența unui divizor prim pozitiv de forma $1+k4$ al lui N, fără a utiliza teoria resturilor pătratice.

Acest lucru se face în felul următor:

Lemă. *Dacă* a *este un număr întreg, atunci* a^2+1 *este un număr întreg de forma* $2^\alpha(4k+1)$, *unde* $\alpha=0$ *sau* $\alpha=1$.

Demonstrație. Dacă a este par avem $a=2u$, deci $a^2+1=4u^2+1=2^0(4u^2+1)$ și prin urmare a^2+1 este de forma $2^\alpha(4k+1)$ cu $\alpha=0$. Dacă a este impar, avem $a=2u+1$, deci $a^2+1=2(2u(u+1)+1)$ și deoarece $u(u+1)$ este totdeauna divizibil cu 2 rezultă că a^2+1 este de forma $2^\alpha(4k+1)$ cu $\alpha=1$.

Lemă. *Dacă* a *este un număr întreg, atunci divizorii primi pozitivi ai numărului întreg* a^2+1 *pot fi numai 2 sau de forma* $1+k4$.

Demonstrație. Vom considera că $a \neq 0$, deoarece dacă $a=0$, atunci a^2+1 este egal cu 1 și nu are divizori primi, deci în acest caz lema este demonstrată.

În cazul cînd $a \neq 0$ vom scrie pe a^2+1 sub forma $2^\alpha(4k+1)$. Dacă $4k+1$ este egal cu 1, atunci a^2+1 poate admite ca divizor prim pozitiv numai pe 2 și lema este demonstrată și în acest caz. Dacă $4k+1$ este diferit de 1, cum $4k+1$ este un număr pozitiv, înseamnă că $4k+1$ este mai mare ca 1, deci $4k+1$ admite un divizor prim pozitiv pe care-l vom nota cu p_1'. Avem deci $4k+1=p_1'M$. Dacă $M=1$, atunci p_1' este de forma $4k+1$ și deci singurii divizori primi pozitivi ai lui a^2+1 pot fi 2 și p_1' și lema este demonstrată și în acest caz. Dacă $M>1$, atunci putem presupune prin absurd că p_1' este de forma $3+k4$, p_1' fiind impar și numerele prime impare neputînd fi decît de forma $1+k4$ sau $3+k4$ cum am demonstrat mai sus. Dar atunci un divizor prim pozitiv al lui M trebuie să fie, de asemenea, de forma $3+k4$, deoarece dacă toți divizorii primi pozitivi ai lui M sînt de forma $1+k4$, atunci și M este de forma $1+k4$, iar $p_1'M$ este de forma $3+k4$, ceea ce contrazice egalitatea $4k+1=p_1'M$. Să presupunem că p_1' este cel mai mic

factor prim pozitiv de forma $3+k4$ din $p_1'M$, iar p_2' este un alt factor prim pozitiv de forma $3+k4$ din același număr $p_1'M$. Avem deci $a^2+1=p_1'p_2'L$, unde $p_1' \leqslant p_2'$ și p_1', p_2' sînt de forma $3+k4$.

Putem avea $2a<p_1'$ sau $2a>p_1'$. Nu putem avea $2a=p_1'$, deoarece 2 nu-l divide pe p_1', p_1' fiind impar. Dacă $2a<p_1'$, atunci avem

$$p_1'p_2'L=a^2+1 \leqslant 2a^2=2aa<p_1'a,$$

deci $p_2'L<a$ și cum $p_1' \leqslant p_2'$, rezultă că $p_1'<a$ sau $p_1'<2a$, ceea ce contrazice relația $2a<p_1'$ admisă ca fiind adevărată. În calculele de mai sus, anume la stabilirea relației $2aa<p^1a$ am presupus că $a>0$, ceea ce se poate admite, deoarece a intervine la pătrat în a^2+1. Apoi, am mai presupus că $a^2 \geqslant 1$, ceea ce rezultă din $a \neq 0$.

Dacă $2a>p_1'$ putem avea $a<p_1'$ sau $a>p_1'$. Nu putem avea $a=p_1'$, deoarece dacă $a=p_1'$, atunci din $a^2+1=p_1'p_2'L$ ar rezulta că p_1' divide pe 1, ceea ce nu se poate. Dacă $a<p_1'$ relația $2a>p_1'$ o putem scrie sub forma $a>p_1'-a>0$ și deci putem defini numărul natural $a'=p_1'-a$ care are proprietatea că $a>a'>0$ și a'^2+1 se divide cu p_1' care este de forma $3+k4$. Dacă $a>p_1'$, cu teorema împărțirii întregi, putem determina două numere întregi q și a' astfel încît $a=p_1'q+a'$ și $0 \leqslant a'<p_1'$. Nu putem avea $a'=0$, deoarece dacă $a'=0$, atunci p_1' divide pe a și deci din $a^2+1=p_1'p_2'L$ rezultă că p_1' divide pe 1, ceea ce nu se poate. Deci $a' \neq 0$ și se constată că a'^2+1 se divide cu p_1', deoarece a^2+1 se divide cu p_1', iar $a'=a-p_1'q$ și se mai constată că $a>a'>0$, deoarece $0<a'<p_1'$ și $p_1'<a$.

În definitiv am demonstrat că dacă numărul întreg a^2+1 are un divizor prim pozitiv de forma $3+k4$, atunci putem determina un număr natural a' astfel încît a'^2+1 să aibă un divizor prim pozitiv de forma $3+k4$, iar $a>a'>0$.

Raționamentul făcut poate fi acum continuat indefinit, deoarece a' se găsește în situația în care se afla a. Dar aceasta înseamnă că putem determina o infinitate de numere naturale a', a'', ... astfel încît $a>a'>a''>\ldots>0$, ceea ce nu se poate. Înlăturarea acestui fapt absurd înseamnă că lema enunțată este demonstrată.

Consecință. *Dacă $a>1$, atunci numărul întreg a^2+1 are un divizor prim pozitiv de forma $1+k4$.*

Într-adevăr, dacă $a>1$, atunci $a^2+1>2$. Dacă a^2+1 nu se divide cu 2, atunci a^2+1, fiind mai mare ca 2, are factori primi care toți sînt de forma $1+k4$, iar dacă a^2+1 se divide cu 2, conform primei leme, a^2+1 nu se divide cu puteri mai mari ale lui 2

și fiindcă $a^2+1>2$, rezultă că a^2+1 are și factori primi impari, care, conform celei de a doua leme, sînt toți de forma $1+k4$, deci consecința este demonstrată.

De aici rezultă că numărul $1+(2p_1 \ldots p_n)^2$ alcătuit mai sus admite un divizor prim pozitiv de forma $1+k4$, deoarece $2p_1 \ldots p_n>1$.

Teoremă. *În progresia aritmetică $1+k6$ există o infinitate de numere prime pozitive.*

Demonstrație. Vom păstra demonstrația dată mai sus acestei teoreme cu singura deosebire că vom demonstra existența unui divizor prim pozitiv de forma $1+k6$ al lui N, fără a utiliza teoria resturilor pătratice.

Acest lucru se face în felul următor:

Lemă. *Dacă a este un număr întreg, atunci a^2+3 este un număr întreg de forma $2^\alpha 3^\beta(6k+1)$, unde $\alpha=0$ sau $\alpha=2$, iar $\beta=0$ sau $\beta=1$.*

Demonstrație. Putem avea următoarele cazuri $a=6u$, $a=6u \pm 1$, $a=6u \pm 2$, $a=6u+3$, ceea ce rezultă prin aplicarea teoremei împărțirii întregi lui a și 6 și prin transformarea convenabilă a resturilor obținute. Dacă $a=6u$ avem $a^2+3=3(6(2u^2)+1)$, deci a^2+3 este de forma $2^\alpha 3^\beta(6k+1)$ cu $\alpha=0$, $\beta=1$. Dacă $a=6u \pm 1$ avem $a^2+3=36u^2 \pm 12u+4=4(9u^2 \pm 3u+1)=4(3u(3u \pm 1)+1)$, deci a^2+3 este de forma $2^\alpha 3^\beta(6k+1)$ cu $\alpha=2$, $\beta=0$, deoarece $u(3u \pm 1)$ este totdeauna divizibil cu 2. Dacă $a=6u \pm 2$ avem $a^2+3=36u^2 \pm \pm 24u+7=6(6u^2 \pm 4u+1)+1$, deci a^2+3 este de forma $2^\alpha 3^\beta(6k+1)$ cu $\alpha=0$, $\beta=0$. Dacă $a=6u+3$ avem $a^2+3=36u^2+36u+12=12(3u(u+1)+1)$, deci a^2+3 este de forma $2^\alpha 3^\beta(6k+1)$ cu $\alpha=2$, $\beta=1$, deoarece $u(u+1)$ este totdeauna divizibil cu 2.

Lemă. *Dacă a este un număr întreg, atunci divizorii primi pozitivi ai numărului întreg a^2+3 pot fi numai 2 sau 3 sau numai de forma $1+k6$.*

Demonstrație. Vom scrie pe a^2+3 sub forma $2^\alpha 3^\beta(6k+1)$. Dacă $6k+1$ este egal cu 1, atunci a^2+3 poate admite ca divizori primi pozitivi numai pe 2 și 3 și lema este demonstrată. Dacă $6k+1$ este diferit de 1, cum $6k+1$ este un număr pozitiv, înseamnă că $6k+1$ este mai mare ca 1, deci $6k+1$ admite un divizor prim pozitiv, pe care-l vom nota cu p_1'. Avem deci $6k+1=p_1'M$. Dacă $M=1$, atunci p_1' este de forma $1+k6$ și deci singurii divizori primi pozitivi ai lui a^2+3 pot fi 2, 3 și p_1' și lema este demonstrată și în acest caz. Dacă $M>1$, atunci putem presupune prin absurd că p_1' este de forma $5+k6$, p_1' fiind diferit de 2 și 3 și numerele

prime pozitive neputînd fi decît de forma $1+k6$ sau $5+k6$, cum am demonstrat mai sus. Dar atunci un divizor prim pozitiv al lui M trebuie să fie, de asemenea, de forma $5+k6$, deoarece dacă toți divizorii primi pozitivi ai lui M sînt de forma $1+k6$, atunci și M este de forma $1+k6$, iar $p_1'M$ este de forma $5+k6$, ceea ce contrazice egalitatea $6k+1=p_1'M$. Să presupunem că p_1' este cel mai mic factor prim pozitiv de forma $5+k6$ din $p_1'M$, iar p_2' este un alt factor prim pozitiv de forma $5+k6$ din același număr $p_1'M$. Avem deci $a^2+3=p_1'p_2'L$, unde $p_1'\leqslant p_2'$ și p_1', p_2' sînt de forma $5+k6$.

Putem avea $2a<p_1'$ sau $2a>p_1'$. Nu putem avea $2a=p_1'$, deoarece 2 nu-l divide pe p_1', p_1' fiind impar. Dacă $2a<p_1'$, atunci avem

$$p_1'p_2'L=a^2+3\leqslant 2a^2=2aa<p_1'a,$$

deci $p_2'L<a$ și cum $p_1'\leqslant p_2'$, rezultă că $p_1'<a$ sau $p_1'<2a$, ceea ce contrazice relația $2a<p_1'$ admisă ca fiind adevărată. În calculele de mai sus, anume la stabilirea relației $2aa<p_1'a$ am presupus că $a>0$, ceea ce se poate admite, deoarece a intervine la pătrat în a^2+3. Apoi am presupus că $a^2\geqslant 3$, ceea ce rezultă din $a^2+3=p_1'p_2'L\geqslant p_1'\geqslant 6\cdot 0+5$, deci $a^2+3\geqslant 5$ sau $a^2\geqslant 2$. Însă $a^2\neq 2$, deci $a^2>2$ sau $a^2\geqslant 3$.

Dacă $2a>p_1'$ putem avea $a<p_1'$ sau $a>p_1'$. Nu putem avea $a=p_1'$, deoarece dacă $a=p_1'$, atunci din $a^2+3=p_1'p_2'L$ ar rezulta că p_1' divide pe 3, deci că $p_1'=3$, ceea ce nu se poate, deoarece 3 nu este de forma $5+k6$. Dacă $a<p_1'$ relația $2a>p_1'$ o putem scrie sub forma $a>p_1'-a>0$ și deci putem defini numărul natural $a'=p_1'-a$ care are proprietatea că $a>a'>0$ și a'^2+3 se divide cu p_1' care este de forma $5+k6$. Dacă $a>p_1'$, cu teorema împărțirii întregi, putem determina două numere întregi q și a' astfel încît $a=p_1'q+a'$ și $0\leqslant a'<p_1'$. Nu putem avea $a'=0$, deoarece dacă $a'=0$, atunci p_1' divide pe a și deci din $a^2+3=p_1'p_2'L$ rezultă că p_1' divide pe 3, deci că $p_1'=3$, ceea ce nu se poate, deoarece 3 nu este de forma $5+k6$. Deci $a'\neq 0$ și se constată că a'^2+3 se divide cu p_1', deoarece a^2+3 se divide cu p_1', iar $a'=a-p_1'q$ și se mai constată că $a>a'>0$, deoarece $0<a'<p_1'$ și $p_1'<a$.

În definitiv am demonstrat că dacă numărul întreg a^2+3 are un divizor prim pozitiv de forma $5+k6$, atunci putem determina un număr natural a' astfel încît a'^2+3 să aibă un divizor prim pozitiv de forma $5+k6$, iar $a>a'>0$.

Raționamentul poate fi acum continuat indefinit, deoarece a' se găsește în situația în care se afla a. Dar aceasta înseamnă că

putem determina o infinitate de numere naturale a', a'', ... astfel încît $a>a'>a''>\ldots>0$, ceea ce nu se poate. Înlăturarea acestui fapt absurd conduce la demonstrarea lemei de mai sus.

Consecință. *Dacă $a>1$ și $a\neq 3$, atunci numărul întreg a^2+3 are un divizor prim pozitiv de forma $1+k6$.*

Demonstrație. Într-adevăr, dacă $a>1$ avem $a^2+3>4$ și dacă $a\neq 3$ și $a<3$ rezultă că $a=2$, deci $a^2+3=2^2+3=7=1+6\cdot 1$, iar dacă $a>3$ avem $a^2+3>12$ și atunci, conform primei leme, rezultă că a^2+3 are și factori primi pozitivi diferiți de 2 și 3 care, conform celei de a doua leme, sînt toți de forma $1+k6$, deci consecința este demonstrată.

De aici rezultă că numărul $3+(2p_1\ldots p_n)^2$ alcătuit mai sus admite un divizor prim pozitiv de forma $1+k6$, deoarece

$$2p_1\ldots p_n>1,\ 2p_1\ldots p_n\neq 3.$$

Capitolul 13

COMPORTARE ASIMPTOTICĂ

13.1. Comportarea asimptotică a funcțiilor reale sau complexe de variabilă reală

In teoria numerelor intervine studiul multor funcții reale sau complexe de variabilă reală în vecinătatea infinitului.

Reamintim că prin funcție reală de variabilă reală se înțelege un ansamblu format din următoarele trei elemente :

(1) o mulțime de numere reale, pe care o vom nota cu E, care se numește *domeniul de definiție al funcției* sau *domeniul funcției* motiv pentru care funcția se numește *de variabilă reală* ;

(2) o mulțime de numere reale, pe care o vom nota cu F, care se numește *domeniul valorilor funcției* sau *codomeniul funcției* motiv pentru care funcția se numește *reală* ;

(3) un procedeu prin care fiecărui număr real $x \in E$ îi corespunde un singur număr real $y \in F$, procedeu numit *corespondență univocă*.

O funcție reală de variabilă reală se notează, de obicei, prin

$$f : E \to F,$$

unde f este *denumirea funcției*, punînd în evidență cele trei elemente prin care este definită funcția f, anume : domeniul, codomeniul și corespondența univocă, ultima fiind reprezentată prin săgeata pusă între domeniu și codomeniu. Notația $f : E \to F$ se citește „funcția f definită pe E cu valori în F“ sau „aplicația f a lui E în F“.

Un mod răspîndit, tradițional și prescurtat de a nota o funcție reală de variabilă reală este următorul : $f(x)$, unde f este denumirea funcției considerate, x este un număr real din mulțimea E, iar numărul real y din F care corespunde lui x este chiar $f(x)$. În această notație, atît mulțimile E și F cît și corespondența care face ca lui x să-i corespundă y se presupun cunoscute. Deci notația $f(x)$ trebuie privită ca fiind egal îndreptățită, ca și notația $f : E \to F$, de a fi utilizată ori de cîte ori este vorba de funcții reale de variabilă reală.

O funcție complexă de variabilă reală se definește analog, cu deosebirea că codomeniul în acest caz este o mulțime de numere complexe, motiv pentru care funcția se numește complexă.

Pentru mai multă conciziune în exprimare, în loc de funcții reale sau complexe de variabilă reală, spunem funcții, adăugîndu-le cîte un adjectiv, cum este cazul funcțiilor numerice care sînt funcții reale sau complexe de variabilă reală pentru care domeniul este mulțimea numerelor întregi sau reale.

În cele ce urmează, vom presupune, ori de cîte ori va fi nevoie, că fiecare din funcțiile considerate are particularitatea că există un număr real x_0 astfel încît orice număr real x care verifică inegalitatea $x \geqslant x_0$ aparține lui E. Cu alte cuvinte, asta înseamnă că funcțiile $f(x)$ considerate sînt definite pentru orice x pentru care $x > x_0$ sau că sînt definite în vecinătatea infinitului.

În cazul unui număr finit de funcții $f_1(x)$, $f_2(x)$, ..., $f_n(x)$ de genul celor de mai sus, există, după cum vom arăta mai jos, un număr real x_f astfel încît $f_i(x)$, oricare ar fi f_i, $i = 1, 2, \ldots, n$, să fie definită pentru orice x pentru care $x > x_f$.

Într-adevăr, nu avem decît să luăm $x_f = \max(x_1, x_2, \ldots, x_n)$, unde x_i corespunde lui $f_i(x)$. Dacă luăm $x > x_f$, atunci $f_i(x)$ va fi definită, deoarece $x > x_f \geqslant x_i$, adică $x > x_i$, funcția $f_i(x)$ fiind definită pentru orice număr real x pentru care $x > x_i$.

Comportarea asimptotică a unei funcții se definește în felul următor :

Definiție. *Fiind date două funcții $f(x)$ și $g(x)$, se spune că funcția $g(x)$ dă comportarea asimptotică a funcției $f(x)$ și se scrie acest lucru astfel*

$$f(x)=O(g(x)),$$

dacă există două constante (numere reale) pozitive C_1 și C_2 astfel încît

$$g(x)>0 \text{ și } |f(x)|<C_1 g(x)$$

pentru orice x pentru care $x>C_2$.

Observație. Relația $f(x)=O(g(x))$ se citește „$f(x)$ este o mare de $g(x)$". Prin $|f(x)|$ trebuie să înțelegem valoarea absolută a lui $f(x)$ în cazul cînd $f(x)$ este o funcție reală sau modulul lui $f(x)$ în cazul cînd $f(x)$ este o funcție complexă.

Consecință. O funcție este mărginită în vecinătatea infinitului dacă și numai dacă

$$f(x)=O(1).$$

Într-adevăr, dacă $f(x)=O(1)$ atunci există două constante pozitive C_1 și C_2 astfel încît $1>0$ și $|f(x)|<C_1\cdot 1$ pentru orice x pentru care $x>C_2$. Rezultă că $|f(x)|<C_1$ pentru orice x pentru care $x>C_2$. Dacă $f(x)$ este o funcție reală, atunci $-C_1<f(x)<C_1$ pentru orice x pentru care $x>C_2$, adică funcția $f(x)$ este mărginită în vecinătatea infinitului. Dacă $f(x)$ este o funcție complexă, atunci $f(x)=h(x)+ik(x)$, $h(x)$ și $k(x)$ fiind funcții reale. Dar $|h(x)|=\sqrt{h^2(x)}\leqslant \sqrt{h^2(x)+k^2(x)}=|f(x)|<C_1$, deci $|h(x)|<C_1$ și tot astfel și $|k(x)|<C_1$ pentru orice x pentru care $x>C_2$, deci funcția $f(x)$ este mărginită în vecinătatea infinitului.

Reciproc, dacă funcția $f(x)$ este reală și mărginită în vecinătatea infinitului înseamnă că există trei constante C_3, C_4 și C_5 astfel încît $C_3<f(x)<C_4$ pentru orice x pentru care $x>C_5$. Dacă notăm cu C_1 o constantă pozitivă astfel încît $C_1\geqslant \max(|C_3|, |C_4|)$, iar cu C_2 o constantă pozitivă astfel încît $C_2\geqslant C_5$, atunci avem $-C_1<f(x)<C_1$ sau $|f(x)|<C_1$ pentru orice x pentru care $x>C_2$. Asta înseamnă că $1>0$ și $|f(x)|<C_1\cdot 1$ pentru orice x pentru care $x>C_2$ deci $f(x)=O(1)$. Dacă funcția $f(x)$ este complexă și mărginită în vecinătatea infinitului, înseamnă că există constantele C_3', C_4', C_5', C_3'', C_4'', C_5'' astfel încît $C_3'<h(x)<C_4'$ pentru orice x pentru care $x>C_5'$ și $C_3''<k(x)<C_4''$ pentru orice x pentru care $x>C_5''$, funcția $f(x)$ punîndu-se sub forma $f(x)=h(x)+ik(x)$,

unde $h(x)$ și $k(x)$ sînt funcții reale. Luînd constantele pozitive C_1 și C_2 astfel încît $\frac{C_1}{\sqrt{2}}\geqslant \max(|C_3'|, |C_4'|, |C_3''|, |C_4''|)$ și $C_2\geqslant \max(C_5', C_5'')$ obținem $|h(x)|<\frac{C_1}{\sqrt{2}}$, $|k(x)|<\frac{C_1}{\sqrt{2}}$ pentru orice x pentru care $x>C_2$, deci $|f(x)|=\sqrt{h^2(x)+k^2(x)}<C_1$ pentru orice x pentru care $x>C_2$. Asta înseamnă că $1>0$ și $|f(x)|<C_1\cdot 1$ pentru orice x pentru care $x>C_2$, deci $f(x)=O(1)$.

Teoremă. *O condiție suficientă ca o funcție $g(x)$ să dea comportarea asimptotică a unei funcții $f(x)$ este ca să existe o constantă (număr real) C_3 astfel încît $g(x)>0$ pentru orice x pentru care $x>C_3$, iar $\lim\limits_{x\to\infty}\frac{|f(x)|}{g(x)}$ să existe și să fie finită.*

Demonstrație. Să notăm $l=\lim\limits_{x\to\infty}\frac{|f(x)|}{g(x)}$. Asta înseamnă că pentru fiecare număr real pozitiv ε există cîte o constantă C_4 astfel încît să avem $\left|\frac{|f(x)|}{g(x)}-l\right|<\varepsilon$ pentru orice x pentru care $x>C_4$. Rezultă că $-\varepsilon<\frac{|f(x)|}{g(x)}-l<\varepsilon$ deci $-\varepsilon+l<\frac{|f(x)|}{g(x)}<l+\varepsilon$ de unde $\frac{f(x)|}{g(x)}<l+\varepsilon$. Putem alege de la început $\varepsilon<1$, deci $\frac{|f(x)|}{g(x)}<l+1$ pentru orice x pentru care $x>C_4$. Dacă notăm cu C_1 o constantă pozitivă astfel încît $l+1\leqslant C_1$ și dacă notăm cu C_2 o constantă pozitivă astfel încît $C_2\geqslant \max(C_3, C_4)$, atunci putem trage concluzia că există două constante pozitive C_1 și C_2 astfel încît

$$g(x)>0 \text{ și } |f(x)|<C_1 g(x),$$

pentru orice x pentru care $x>C_2$, ceea ce înseamnă că $f(x)=O(g(x))$.

Observație. Condiția nu este necesară, deoarece cu $f(x)=\sin x$ și $g(x)=1$ este realizată comportarea asimptotică $\sin x=O(1)$, deoarece funcția $\sin x$ este mărginită în vecinătatea infinitului, dar $\lim\limits_{x\to\infty}\frac{|\sin x|}{1}$ nu există.

Exemple.

(1) $2x+\sqrt{x}=O(x)$,

deoarece luînd $C_3=0$ în formularea teoremei de mai sus, obținem $x>0$ pentru orice x pentru care $x>C_3$, iar $\lim\limits_{x\to\infty}\frac{|2x+\sqrt{x}|}{x}=\lim\limits_{x\to\infty}\frac{2x+\sqrt{x}}{x}=$ $=\lim\limits_{x\to\infty}(2+\frac{1}{\sqrt{x}})=2$ este finită.

(2) $x(x-3)^{-1}=O(1)$,

deoarece oricum l-am lua pe C_3 în formularea teoremei de mai sus, obținem $1>0$, iar $\lim\limits_{x\to\infty}\frac{|x(x-3)^{-1}|}{1}=\lim\limits_{x\to\infty}\frac{x}{x-3}=1$ este finită.

(3) $\log(x+h)=\log x+\frac{h}{x}+O\left(\frac{1}{x^2}\right)$, *unde* h *este o constantă.*

Într-adevăr, conform formulei lui Taylor, pentru o funcție $f(x)$ care admite primele două derivate, avem

$$f(x+h)=f(x)+hf'(x)+\frac{h^2f''(x+\theta h)}{2!},\quad 0<\theta<1,$$

h fiind o constantă. Luînd $f(x)=\log x$, obținem $f'(x)=\frac{1}{x}$, $f''(x)=$ $=-\frac{1}{x^2}$. Avem

$$\lim_{x\to\infty}\frac{\frac{h^2f''(x+\theta h)}{2!}}{\frac{1}{x^2}}=\lim_{x\to\infty}\frac{-h^2x^2}{2!(x+\theta h)^2}=\lim_{x\to\infty}\frac{-h^2}{2!\left(1+\frac{\theta h}{x}\right)^2}=-\frac{h^2}{2}$$

care este finită. Luînd $C_3=0$ în formularea teoremei precedente avem $\frac{1}{x^2}>0$ pentru orice $x>C_3$ deci $\frac{h^2f''(x+\theta h)}{2!}=O\left(\frac{1}{x^2}\right)$ atunci cînd $f(x)=\log x$. Deci proprietatea (3) este demonstrată.

13.2. Cîteva proprietăți ale comportării asimptotice

(1) *Dacă* $f(x)=CO(g(x))$, *iar* C *este o constantă, atunci* $f(x)=$ $=O(g(x))$.

Demonstrație. Vom scrie $f(x)=Ch(x)$, unde $h(x)=O(g(x))$. *Există* două constante pozitive C_1 și C_2 astfel încît $g(x)>0$ și $|h(x)|<$ $<C_1g(x)$ pentru orice x pentru care $x>C_2$. Atunci $|f(x)|=|C||h(x)|\leqslant$ $\leqslant(|C|C_1)g(x)$, egalitatea avînd loc numai dacă $C=0$. Notînd cu C_1' o constantă pozitivă astfel încît $C_1'\geqslant|C|C_1$, constatăm că există două constante pozitive C_1' și C_2 astfel încît $g(x)>0$ și $|f(x)|<C_1'g(x)$ pentru orice x pentru care $x>C_2$, deci $f(x)=O(g(x))$.

(2) *Dacă* $f(x)=k(x)O(g(x))$ *și există un număr real* x_k *astfel încît* $k(x)\neq0$ *pentru orice* x *pentru care* $x>x_k$, *atunci* $f(x)=O(|k(x)|g(x))$.

Demonstrație. Vom scrie $f(x)=k(x)h(x)$, unde $h(x)=O(g(x))$. Există două constante pozitive C_1 și C_2 astfel încît $g(x)>0$ și $|h(x)|<C_1g(x)$ pentru orice x pentru care $x>C_2$. Atunci $|f(x)|=$ $=|k(x)||h(x)|<C_1(|k(x)|g(x))$ pentru orice x pentru care $x>\max(C_2,$ $x_k)$. Notînd $C_2'=\max(C_2,\ x_k)$, constatăm că C_2' este o constantă pozitivă și că $|k(x)|g(x)>0$ și $|f(x)|<C_1(|k(x)|g(x))$ pentru orice x pentru care $x>C_2'$, deci $f(x)=O(|k(x)|g(x))$.

(3) *Dacă* $f_1(x)=O(g(x))$, ..., $f_n(x)=O(g(x))$, n *fiind un număr natural, atunci* $f_1(x)+\ldots+f_n(x)=O(g(x))$.

Demonstrație. Pentru fiecare $i=1,\ \ldots,\ n$ există cîte două constante pozitive C_{1i} și C_{2i} astfel încît $g(x)>0$ și $|f_i(x)|<C_{1i}g(x)$ pentru orice $x>C_{2i}$. Ținînd seama de $|f_1(x)+\ldots+f_n(x)|\leqslant|f_1(x)|+$ $\ldots+|f_n(x)|$ și luînd $C_1=C_{11}+\ldots+C_{1n}$ și $C_2=\max(C_{21},\ \ldots,C_{2n})$ obținem că $g(x)>0$ și $|f_1(x)+\ldots+f_n(x)|<C_1g(x)$ pentru orice x pentru care $x>C_2$, deci $f_1(x)+\ldots+f_n(x)=O(g(x))$.

(4) *Dacă* $f(x)=O(g(x))$, *atunci* $|f(x)|=O(g(x))$.

Demonstrație. Deoarece $f(x)=O(g(x))$ există două constante pozitive C_1 și C_2 astfel încît $g(x)>0$ și $|f(x)|<C_1g(x)$ pentru orice x pentru care $x>C_2$, adică astfel încît $g(x)>0$ și $||f(x)||<C_1g(x)$ pentru orice x pentru care $x>C_2$, deci $|f(x)|=O(g(x))$.

(5) *Dacă* $|f(x)| \leqslant O(g(x))$ *atunci* $f(x)=O(g(x))$.

Demonstrație. Vom scrie $|f(x)| \leqslant h(x)$, unde $h(x)=O(g(x))$. Există două constante pozitive C_1 și C_2 astfel încît $g(x)>0$ și $|h(x)|<C_1 g(x)$ pentru orice x pentru care $x>C_2$. Rezultă că $|f(x)| \leqslant h(x)=|h(x)|<C_1 g(x)$, deci $g(x)>0$ și $|f(x)|<C_1 g(x)$ pentru orice x pentru care $x>C_2$, de unde rezultă că $f(x)=O(g(x))$.

(6) *Dacă* $f(x)=O(g(x))$ *și* $g(x)=O(h(x))$ *atunci* $f(x)=O(h(x))$.

Demonstrație. Există două constante pozitive C_1 și C_2 astfel încît $h(x)>0$ și $|g(x)|<C_1 h(x)$ pentru orice x pentru care $x>C_2$ și mai există două constante pozitive C_3 și C_4 astfel încît $g(x)>0$ și $|f(x)|<C_3 g(x)$ pentru orice x pentru care $x>C_4$. Deci $|f(x)|<C_3 g(x)=C_3|g(x)|<(C_1 C_3)h(x)$ pentru orice x pentru care $x>\max(C_2, C_4)$. Punînd $C_5=C_1 C_3$ și $C_6=\max(C_2, C_4)$ înseamnă că există două constante pozitive C_5 și C_6 astfel încît $h(x)>0$ și $|f(x)|<C_5 h(x)$ pentru orice x pentru care $x>C_6$, deci $f(x)=O(h(x))$.

(7) *Fiind date funcțiile* $f(x)$, $g(x)$ *și* $h(x)$ *astfel încît*:
(a) *să fie definite pentru orice număr natural* x,
(b) *să existe un număr natural* a *pentru care* $f(a)g(a)\neq 0$,
(c) *iar* $h(x)=O(g(x))$,
atunci

$$\sum_{1\leqslant n\leqslant x} f(n)h(n)=O\Big(\sum_{1\leqslant n\leqslant x}|f(n)||g(n)|\Big),$$

sumele fiind extinse la mulțimea numerelor naturale cel mult egale cu un număr real x, *fiecare număr natural din această mulțime fiind luat o singură dată.*

Demonstrație. Există două constante pozitive C_1 și C_2 astfel încît

$$g(x)>0 \text{ și } |h(x)|<C_1 g(x)$$

pentru orice x pentru care $x>C_2$. Dacă C_2' este o constantă astfel încît $C_2'=\max(C_2, a)$, atunci vom scrie

$$\Big|\sum_{1\leqslant n\leqslant x} f(n)h(n)\Big| \leqslant \sum_{1\leqslant n\leqslant C_2'}|f(n)||h(n)|+\sum_{C_2'<n\leqslant x}|f(n)||h(n)|<$$

$$<\sum_{1\leqslant n\leqslant C_2'}|f(n)||h(n)|+C_1\sum_{C_2'<n\leqslant x}|f(n)||g(n)|,$$

deoarece pentru $n>C_2'$ avem și $n>C_2$ și deci $g(n)>0$ și $|h(n)|<C_1 g(n)=C_1|g(n)|$. Dar

$$\sum_{1\leqslant n\leqslant C_2'}|f(n)||g(n)|\neq 0,$$

deoarece $a\leqslant C_2'$, iar $f(a)g(a)\neq 0$. Punînd

$$C_3=\frac{\sum\limits_{1\leqslant n\leqslant C_2'}|f(n)||h(n)|}{\sum\limits_{1\leqslant n\leqslant C_2'}|f(n)||g(n)|}$$

obținem

$$\Big|\sum_{1\leqslant n\leqslant x} f(n)h(n)\Big|<C_3\sum_{1\leqslant n\leqslant C_2'}|f(n)||g(n)|+C_1\sum_{C_2'<n\leqslant x}|f(n)||g(n)|.$$

Dacă $C_1'=\max(C_1, C_3)$ atunci există două constante pozitive C_1', C_2' astfel încît

$$\sum_{1\leqslant n\leqslant x}|f(n)||g(n)|>0, \Big|\sum_{1\leqslant n\leqslant x} f(n)h(n)\Big|<C_1'\sum_{1\leqslant n\leqslant x}|f(n)||g(n)|$$

pentru orice x pentru care $x>C_2'$, deci rezultă că

$$\sum_{1\leqslant n\leqslant x} f(n)h(n)=O\Big(\sum_{1\leqslant n\leqslant x}|f(n)||g(n)|\Big).$$

Funcțiile $f(x)$, $g(x)$ și $h(x)$ trebuie să fie definite pentru orice număr natural x pentru ca sumele considerate să aibă sens.

(8) *Fiind date funcțiile* $f(x)$, $g(x)$ *și* $h(x)$ *astfel încît*:
(a) $f(x)$ *să fie definită pentru orice număr natural* x, $g(x)$ *să fie definită, iar* $h(x)$ *să fie definită și mărginită pe intervalul* $[1, \alpha]$, *pentru orice* α *pentru care* $\alpha\geqslant 1$,
(b) *pe intervalul* $[1, \alpha]$, *să existe un număr real pozitiv* m *astfel încît* $|g(x)|\geqslant m$ *pentru orice* α *real pentru care* $\alpha\geqslant 1$ *și să existe un număr natural* a *pentru care* $f(a)\neq 0$,
(c) $h(x)=O(g(x))$,
atunci

$$\sum_{1\leqslant n\leqslant x} f(n)h\left(\frac{x}{n}\right)=O\Big(\sum_{1\leqslant n\leqslant x}|f(n)|\Big|g\left(\frac{x}{n}\right)\Big|\Big),$$

sumele fiind extinse la mulțimea numerelor naturale cel mult egale cu un număr real x, *fiecare număr natural din această mulțime fiind luat o singură dată.*

Demonstrație. Există două constante pozitive C_1 și C_2 astfel încît

$$g(x)>0 \text{ și } |h(x)|<C_1 g(x)$$

pentru orice x pentru care $x>C_2$. Din această cauză vom scrie

$$\left|\sum_{1\leqslant n\leqslant x} f(n)h\left(\frac{x}{n}\right)\right| \leqslant \sum_{1\leqslant n<\frac{x}{C_2}} |f(n)|\left|h\left(\frac{x}{n}\right)\right| + \sum_{\frac{x}{C_2}\leqslant n\leqslant x} |f(n)|\left|h\left(\frac{x}{n}\right)\right|.$$

Atunci cînd $1\leqslant n<\frac{x}{C_2}$, avem $C_2<\frac{x}{n}$ deci

$$\sum_{1\leqslant n<\frac{x}{C_2}} |f(n)|\left|h\left(\frac{x}{n}\right)\right| < C_1 \sum_{1\leqslant n<\frac{x}{C_2}} |f(n)|\left|g\left(\frac{x}{n}\right)\right|.$$

Atunci cînd $\frac{x}{C_2}\leqslant n\leqslant x$, avem $1\leqslant\frac{x}{n}\leqslant C_2$ și deci există un număr real M astfel încît pentru $1\leqslant\frac{x}{n}\leqslant C_2$ să avem

$$\left|h\left(\frac{x}{n}\right)\right|\leqslant M,$$

deoarece funcția $h(x)$ este mărginită pe intervalul $[1\ C_2]$. Există un număr real pozitiv m astfel încît pentru orice x pentru care $1\leqslant\frac{x}{n}\leqslant C_2$ să avem

$$\left|g\left(\frac{x}{n}\right)\right|\geqslant m.$$

Deci

$$\sum_{\frac{x}{C_2}\leqslant n\leqslant x} |f(n)|\left|h\left(\frac{x}{n}\right)\right| \leqslant \frac{M}{m} \sum_{\frac{x}{C_2}\leqslant n\leqslant x} |f(n)|\left|g\left(\frac{x}{n}\right)\right|.$$

Dacă punem $C_2'=a$, atunci pentru orice x pentru care $x>C_2'$ avem

$$\sum_{1\leqslant n\leqslant x} |f(n)|\left|g\left(\frac{x}{n}\right)\right|>0,$$

deoarece în această sumă figurează termenul $|f(a)|\left|g\left(\frac{x}{a}\right)\right|$ care este diferit de zero pe motivul că $f(a)\neq 0$ și $g\left(\frac{x}{a}\right)\neq 0$, deoarece $\frac{x}{a}\geqslant 1$. Dacă mai notăm $C_1'=\max\left(C_1,\frac{M}{m}\right)$ atunci înseamnă că există două constante pozitive C_1' și C_2' astfel încît

$$\sum_{1\leqslant n\leqslant x}\left|f(n)\right|\left|g\left(\frac{x}{n}\right)\right|>0 \quad \text{și} \quad \left|\sum_{1\leqslant n\leqslant x} f(n)h\left(\frac{x}{n}\right)\right| < C_1' \sum_{1\leqslant n\leqslant x}\left|f(n)\right|\left|g\left(\frac{x}{n}\right)\right|$$

pentru orice x pentru care $x>C_2'$, deci proprietatea (8) este demonstrată.

13.3. Cazuri particulare de comportare asimptotică

Primul caz particular de comportare asimptotică. Dacă există o constantă C_3 astfel încît $g(x)>0$ pentru orice x pentru care $x>C_3$, iar $\lim\limits_{x\to\infty}\frac{f(x)}{g(x)}=0$, atunci se scrie

$$f(x)=o(g(x))$$

și se citește „$f(x)$ este o mic de $g(x)$“.

Observație. Avem într-adevăr un caz particular de comportare asimptotică, deoarece dacă $f(x)=o(g(x))$ atunci $f(x)=O(g(x))$, dar nu și reciproc.

Acest lucru rezultă în felul următor. Din $f(x)=o(g(x))$ rezultă că există o constantă C_3 astfel încît să avem $g(x)>0$ pentru orice x pentru care $x>C_3$, iar $\lim\limits_{x\to\infty}\frac{f(x)}{g(x)}=0$. Dar atunci $\lim\limits_{x\to\infty}\frac{|f(x)|}{g(x)}=$ $=\left|\lim\limits_{x\to\infty}\frac{f(x)}{g(x)}\right|=0$.

Deci $f(x)=O(g(x))$. Reciproca nu este adevărată, adică din $f(x)=O(g(x))$ nu rezultă că $f(x)=o(g(x))$, deoarece $\lim\limits_{x\to\infty}\frac{|f(x)|}{g(x)}$ s-ar putea să nu existe sau dacă există, s-ar putea ca $\lim\limits_{x\to\infty}\frac{f(x)}{g(x)}\neq 0$. Dar acest lucru contrazice că $f(x)=o(g(x))$, deoarece din $f(x)=o(g(x))$ rezultă că $\lim\limits_{x\to\infty}\frac{f(x)}{g(x)}=0$ și deci rezultă, ca mai sus, că $\lim\limits_{x\to\infty}\frac{|f(x)|}{g(x)}=0$.

Consecință. $\lim\limits_{x\to\infty} f(x)=0$ *dacă și numai dacă*

$$f(x)=o(1).$$

Într-adevăr, dacă $f(x)=o(1)$, atunci există o constantă C_3 astfel încît $1>0$ pentru orice x pentru care $x\geqslant C_3$, iar $\lim\limits_{x\to\infty}\frac{f(x)}{1}=0$, deci $\lim\limits_{x\to\infty} f(x)=0$. Reciproc, dacă $\lim\limits_{x\to\infty} f(x)=0$, atunci luînd drept constanta C_3 un număr real oarecare, vom avea $1>0$ pentru orice x pentru care $x\geqslant C_3$, iar $\lim\limits_{x\to\infty}\frac{f(x)}{1}=0$, deci $f(x)=o(1)$.

Exemple.

(1) $x=o(x^2)$,

deoarece luînd drept constanta C_3 numărul 0, avem $x^2>0$ pentru orice x pentru care $x>C_3$ și apoi $\lim\limits_{x\to\infty}\frac{x}{x^2}=\lim\limits_{x\to\infty}\frac{1}{x}=0$.

(2) $\sin x=o(\sqrt{x})$,

deoarece luînd $C_3=0$, avem $\sqrt{x}>0$ pentru orice x pentru care $x\geqslant C_3$ și apoi $\lim\limits_{x\to\infty}\frac{\sin x}{\sqrt{x}}=0$.

(3) $\log^{\alpha}x=o(x^{\beta})$, *unde* α *și* β *sînt numere reale, iar* $\beta>0$.

Într-adevăr, luînd $C_3=0$ avem $x^{\beta}>0$ pentru orice x pentru care $x>C_3$. Apoi, dacă $\alpha\leqslant 0$, avem $\lim\limits_{x\to\infty}\frac{\log^{\alpha}x}{x^{\beta}}=\lim\limits_{x\to\infty}\frac{1}{x^{\beta}\log^{-\alpha}x}=0$,

iar dacă $\alpha>0$, avem $\lim\limits_{x\to\infty}\frac{\log^{\alpha}x}{x^{\beta}}=\lim\limits_{x\to\infty}\left(\frac{\log x}{x^{\frac{\beta}{\alpha}}}\right)^{\alpha}=\left(\lim\limits_{x\to\infty}\frac{\log x}{x^{\frac{\beta}{\alpha}}}\right)^{\alpha}=$

$$=\left(\lim_{x\to\infty}\frac{\frac{1}{x}}{\frac{\beta}{\alpha}x^{\frac{\beta}{\alpha}-1}}\right)^{\alpha}=\left(\lim_{x\to\infty}\frac{\alpha}{\beta x^{\alpha}}\right)^{\alpha}=0.$$

Deci $\lim\limits_{x\to\infty}\frac{\log^{\alpha}x}{x^{\beta}}=0$ și deci $\log^{\alpha}x=o(x^{\beta})$.

(4) $\frac{1}{\log(x+h)}=\frac{1}{\log x}-\frac{h}{x\log^2 x}+o\left(\frac{1}{x^2}\right)$, *unde* h *este o constantă.*

Într-adevăr, conform formulei lui Taylor pentru o funcție $f(x)$ care admite primele două derivate avem

$$f(x+h)=f(x)+hf'(x)+\frac{h^2f''(x+\theta h)}{2!},\quad 0<\theta<1,$$

h fiind o constantă. Luînd $f(x)=\frac{1}{\log x}$, obținem $f'(x)=-\frac{1}{x\log^2 x}$,

$f''(x)=\frac{\log x+2}{x^2\log^3 x}$. Avem

$$\lim_{x\to\infty}\frac{\frac{h^2f''(x+\theta h)}{2!}}{\frac{1}{x^2}}=\lim_{x\to\infty}\frac{h^2x^2(\log(x+\theta h)+2)}{2(x+\theta h)^2\log^3(x+\theta h)}=$$

$$=\lim_{x\to\infty}\frac{h^2\left(1+\frac{2}{\log(x+\theta h)}\right)}{2\left(1+\frac{\theta h}{x}\right)^2\log^2(x+\theta h)}=0.$$

Luînd $C_3=0$ avem $\frac{1}{x^2}>0$ pentru orice x pentru care $x\geqslant C_3$ deci $\frac{h^2f''(x+\theta h)}{2!}=o\left(\frac{1}{x^2}\right)$ atunci cînd $f(x)=\frac{1}{\log x}$. Deci proprietatea (4) este demonstrată.

Cîteva proprietăţi ale comportării asimptotice o mic.

(1) *Dacă* $f(x)=Co(g(x))$, *iar* C *este o constantă, atunci* $f(x)=o(g(x))$.

Demonstraţie. Vom scrie $f(x)=Ch(x)$, unde $h(x)=o(g(x))$. Există o constantă C_3 astfel încît $g(x)>0$ pentru orice x pentru care $x>C_3$, iar $\lim_{x\to\infty}\frac{h(x)}{g(x)}=0$, deci $\lim_{x\to\infty}\frac{f(x)}{g(x)}=\lim_{x\to\infty}\frac{Ch(x)}{g(x)}=C\lim_{x\to\infty}\frac{h(x)}{g(x)}=0$, deci $f(x)=o(g(x))$,

(2) *Dacă* $f(x)=k(x)o(g(x))$ *şi există un număr real* x_k *astfel încît* $k(x)\neq 0$ *pentru orice* x *pentru care* $x>x_k$, *atunci* $f(x)=o(|k(x)|g(x))$.

Demonstraţie. Vom scrie $f(x)=k(x)h(x)$, unde $h(x)=o(g(x))$. Există o constantă C_3 astfel încît $g(x)>0$ pentru orice x pentru care $x>C_3$, iar $\lim_{x\to\infty}\frac{h(x)}{g(x)}=0$. Avem $-|k(x)h(x)|\leqslant k(x)h(x)\leqslant |k(x)h(x)|$, iar pentru $x>x_k$, deoarece $k(x)\neq 0$, avem $-|h(x)|\leqslant \frac{k(x)h(x)}{|k(x)|}\leqslant |h(x)|$. Dacă avem şi $x>C_3$, adică $x>\max(C_3, x_k)$, atunci $-\frac{|h(x)|}{g(x)}\leqslant\frac{f(x)}{|k(x)|g(x)}\leqslant\frac{|h(x)|}{g(x)}$. Din cauză că $\lim_{x\to\infty}\frac{|h(x)|}{g(x)}=\left|\lim_{x\to\infty}\frac{h(x)}{g(x)}\right|=0$ înseamnă că $\lim_{x\to\infty}\frac{f(x)}{|k(x)|g(x)}$ există şi este egală cu 0. Deci luînd $C_3'=\max(C_3, x_k)$, obţinem că pentru orice x pentru care $x>C_3'$ avem $|k(x)|\,g(x)>0$, iar $\lim_{x\to\infty}\frac{f(x)}{|k(x)|g(x)}=0$, deci $f(x)=o(|k(x)|\,g(x))$.

(3) *Dacă* $f_1(x)=o(g(x)), \ldots, f_n(x)=o(g(x))$, n *fiind un număr natural, atunci* $f_1(x)+\ldots+f_n(x)=o(g(x))$.

Demonstraţie. Pentru fiecare $i=1, \ldots, n$ există cîte o constantă C_{3i} astfel încît $g(x)>0$ pentru orice x pentru care $x>C_{3i}$, iar $\lim_{x\to\infty}\frac{f_i(x)}{g(x)}=0$. Luînd $C_3=\max(C_{31}, \ldots, C_{3n})$ obţinem $g(x)>0$ pentru orice x pentru care $x>C_3$, iar $\lim_{x\to\infty}\frac{f_1(x)+\ldots+f_n(x)}{g(x)}=\lim_{x\to\infty}\frac{f_1(x)}{g(x)}+$

$+\ldots+\lim_{x\to\infty}\frac{f_n(x)}{g(x)}=0$, deci $f_1(x)+\ldots+f_n(x)=o(g(x))$.

(4) *Dacă* $f(x)=o(g(x))$ *atunci* $|f(x)|=o(g(x))$.

Demonstraţie. Deoarece $f(x)=o(g(x))$, există o constantă C_3 astfel încît $g(x)>0$ pentru orice x pentru care $x>C_3$, iar $\lim_{x\to\infty}\frac{f(x)}{g(x)}=0$, deci $\lim_{x\to\infty}\frac{|f(x)|}{g(x)}=\left|\lim_{x\to\infty}\frac{f(x)}{g(x)}\right|=0$, deci $|f(x)|=o(g(x))$.

(5) *Dacă* $|f(x)|\leqslant o(g(x))$ *atunci* $f(x)=o(g(x))$.

Demonstraţie. Vom scrie $|f(x)|\leqslant h(x)$, unde $h(x)=o(g(x))$. Există o constantă C_3 astfel încît $g(x)>0$ pentru orice x pentru care $x>C_3$, iar $\lim_{x\to\infty}\frac{h(x)}{g(x)}=0$. Avem $0\leqslant|f(x)|\leqslant h(x)$, deci $0\leqslant\frac{|f(x)|}{g(x)}\leqslant\frac{h(x)}{g(x)}$ pentru orice x pentru care $x>C_3$. Rezultă că $\lim_{x\to\infty}\frac{|f(x)|}{g(x)}$ există şi este egală cu 0. Deci $f(x)=o(g(x))$, pentru că există o constantă C_3 astfel încît $g(x)>0$ pentru orice x pentru care $x>C_3$ şi $\lim_{x\to\infty}\frac{f(x)}{g(x)}=0$, fiindcă $-|f(x)|\leqslant f(x)\leqslant|f(x)|$, deci $-\frac{|f(x)|}{g(x)}\leqslant\frac{f(x)}{g(x)}\leqslant\frac{|f(x)|}{g(x)}$ pentru orice x pentru care $x>C_3$.

(6) *Dacă* $f(x)=O(g(x))$ *şi* $g(x)=o(h(x))$ *atunci* $f(x)=o(h(x))$.
Dacă $f(x)=o(g(x))$ *şi* $g(x)=O(h(x))$ *atunci* $f(x)=o(h(x))$.
Dacă $f(x)=o(g(x))$ *şi* $g(x)=o(h(x))$ *atunci* $f(x)=o(h(x))$.

Demonstraţie. Dacă $f(x)=O(g(x))$ şi $g(x)=o(h(x))$ atunci există două constante pozitive C_1 şi C_2 astfel încît $g(x)>0$ şi $|f(x)|<C_1g(x)$ pentru orice x pentru care $x>C_2$ şi există o constantă C_3 astfel încît $h(x)>0$ pentru orice x pentru care $x>C_3$, iar $\lim_{x\to\infty}\frac{g(x)}{h(x)}=0$. Rezultă $0\leqslant|f(x)|<C_1g(x)$ pentru orice x pentru care $x>C_2$ şi $0\leqslant\frac{|f(x)|}{h(x)}\leqslant C_1\frac{g(x)}{h(x)}$ dacă şi $x>C_3$, deci dacă $x>\max(C_2, C_3)$.

Dar atunci $\lim_{x\to\infty}\frac{|f(x)|}{h(x)}=0$. Deci $f(x)=o(h(x))$, pentru că există o constantă C_3 astfel încît $h(x)>0$ pentru orice x pentru care $x>C_3$ și $\lim_{x\to\infty}\frac{f(x)}{h(x)}=0$, fiindcă $-|f(x)|\leqslant f(x)\leqslant|f(x)|$, deci $-\frac{|f(x)|}{h(x)}\leqslant\frac{f(x)}{h(x)}\leqslant\frac{|f(x)|}{h(x)}$ pentru orice x pentru care $x>C_3$.

Dacă $f(x)=o(g(x))$ și $g(x)=O(h(x))$ atunci există două constante pozitive C_1 și C_2 astfel încît $h(x)>0$ și $|g(x)|<C_1h(x)$ pentru orice x pentru care $x\geqslant C_2$ și există o constantă C_3 astfel încît $g(x)>0$ pentru orice x pentru care $x>C_3$, iar $\lim_{x\to\infty}\frac{f(x)}{g(x)}=0$. Deoarece $0\leqslant\frac{|f(x)|}{h(x)}=\frac{|f(x)|}{|g(x)|}\frac{|g(x)|}{h(x)}\leqslant C_1\frac{|f(x)|}{g(x)}$ pentru orice x pentru care $x>\max(C_2, C_3)$, rezultă că $\lim_{x\to\infty}\frac{|f(x)|}{h(x)}=0$. Din $-|f(x)|\leqslant f(x)\leqslant|f(x)|$, deci din $-\frac{|f(x)|}{h(x)}\leqslant\frac{f(x)}{h(x)}\leqslant\frac{|f(x)|}{h(x)}$ care are loc pentru orice x pentru care $x>C_2$, obținem $\lim_{x\to\infty}\frac{f(x)}{g(x)}=0$. Deoarece există o constantă C_2 astfel încît $h(x)>0$ pentru orice x pentru care $x>C_2$ și $\lim_{x\to\infty}\frac{f(x)}{h(x)}=0$ înseamnă că $f(x)=o(h(x))$.

Dacă $f(x)=o(g(x))$ și $g(x)=o(h(x))$ rezultă că există o constantă C_3 astfel încît $g(x)>0$ pentru orice x pentru care $x>C_3$, iar $\lim_{x\to\infty}\frac{f(x)}{g(x)}=0$ și există o constantă C_4 astfel încît $h(x)>0$ pentru orice x pentru care $x>C_4$, iar $\lim_{x\to\infty}\frac{g(x)}{h(x)}=0$. Dar $\lim_{x\to\infty}\frac{f(x)}{h(x)}=\lim_{x\to\infty}\frac{f(x)}{g(x)}\cdot\lim_{x\to\infty}\frac{g(x)}{h(x)}=0$ și cum există o constantă C_4 astfel încît $h(x)>0$ pentru orice x pentru care $x>C_4$ rezultă că $f(x)=o(h(x))$.

(7) *Fiind date funcțiile $f(x)$, $g(x)$ și $h(x)$ astfel încît:*
(a) *să fie definite pentru orice număr natural x,*
(b) *seria* $\sum_{n=1}^{\infty}|f(n)||g(n)|$ *să fie divergentă,*

(c) *iar* $h(x)=o(g(x))$,
atunci

$$\sum_{1\leqslant n\leqslant x}f(n)h(n)=o\Big(\sum_{1\leqslant n\leqslant x}|f(n)||g(n)|\Big),$$

sumele fiind extinse la mulțimea numerelor naturale cel mult egale cu un număr real x, fiecare număr natural din această mulțime fiind luat o singură dată.

Demonstrație. Din cauză că $h(x)=o(g(x))$, există o constantă C_1 astfel încît $g(x)>0$, iar $\lim_{x\to\infty}\frac{h(x)}{g(x)}=0$. Deci fiind dat un număr real $\frac{\varepsilon}{2}$ pozitiv, există o constantă C_2, $C_2\geqslant C_1$, astfel încît $\left|\frac{h(x)}{g(x)}-0\right|<\frac{\varepsilon}{2}$ pentru orice x pentru care $x\geqslant C_2$, de unde rezultă că $|h(x)|<\frac{\varepsilon}{2}|g(x)|$ pentru orice x pentru care $x\geqslant C_2$. Din această cauză vom scrie

$$\Big|\sum_{1\leqslant n\leqslant x}f(n)h(n)\Big|\leqslant\sum_{1\leqslant n\leqslant C_2}|f(n)||h(n)|+\sum_{C_2<n\leqslant x}|f(n)||h(n)|<$$
$$<\sum_{1\leqslant n\leqslant C_2}|f(n)||h(n)|+\frac{\varepsilon}{2}\sum_{C_2<n\leqslant x}|f(n)||g(n)|\leqslant$$
$$\leqslant\sum_{1\leqslant n\leqslant C_2}|f(n)||h(n)|+\frac{\varepsilon}{2}\sum_{1\leqslant n\leqslant x}|f(n)||g(n)|.$$

Seria $\sum_{n=1}^{\infty}|f(n)||g(n)|$ fiind divergentă, rezultă că există o constantă C_3 astfel încît pentru orice x pentru care $x\geqslant C_3$ să avem

$$\frac{2}{\varepsilon}\sum_{1\leqslant n\leqslant C_2}|f(n)||h(n)|<\sum_{1\leqslant n\leqslant x}|f(n)||g(n)|$$

din cauză că atunci cînd ε este dat, numărul $\frac{2}{\varepsilon}\sum_{1\leqslant n\leqslant C_2}|f(n)||h(n)|$

este o constantă. Deci pentru fiecare ε real pozitiv avem

$$\left|\sum_{1\leqslant n\leqslant x} f(n)h(n)\right| < \frac{\varepsilon}{2}\sum_{1\leqslant n\leqslant x}|f(n)||g(n)| + \frac{\varepsilon}{2}\sum_{1\leqslant n\leqslant x}|f(n)||g(n)| =$$

$$= \varepsilon \sum_{1\leqslant n\leqslant x}|f(n)||g(n)|$$

pentru orice x pentru care $x > C_3$. Aceasta înseamnă că

$$\lim_{x\to\infty} \frac{\sum_{1\leqslant n\leqslant x} f(n)h(n)}{\sum_{1\leqslant n\leqslant x}|f(n)|\,|g(n)|} = 0.$$

Apoi, din faptul că seria $\sum_{n=1}^{\infty}|f(n)||g(n)|$ este divergentă, înseamnă că fiind dat un număr real și pozitiv m, există o constantă C_4 astfel încît

$$\sum_{1\leqslant n\leqslant x}|f(n)||g(n)| > m$$

pentru orice x pentru care $x \geqslant C_4$, deci

$$\sum_{1\leqslant n\leqslant x}|f(n)||g(n)| > 0$$

pentru orice x pentru care $x > C_4$. Deci proprietatea (7) este demonstrată. Funcțiile $f(x)$, $g(x)$ și $h(x)$ trebuie să fie definite pentru orice număr natural x pentru ca sumele considerate să aibă sens.

Al doilea caz particular de comportare asimptotică. Dacă există o constantă C_3 astfel încît $g(x) > 0$ pentru orice x pentru care $x \geqslant C_3$, iar $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$, atunci se scrie

$$f(x) \sim g(x)$$

și se citește „$f(x)$ este asimptotic egală cu $g(x)$" sau „$f(x)$ și $g(x)$ sînt asimptotic egale".

Observație. Avem într-adevăr un caz particular de comportare asimptotică, deoarece dacă $f(x) \sim g(x)$ atunci $f(x) = O(g(x))$, dar nu și reciproc.

Aceasta rezultă în felul următor. Din $f(x) \sim g(x)$ rezultă că există o constantă C_3 astfel încît să avem $g(x) > 0$ pentru orice x pentru care $x > C_3$, iar $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$. Dar atunci $\lim_{x\to\infty} \frac{|f(x)|}{g(x)} = \left|\lim_{x\to\infty} \frac{f(x)}{g(x)}\right| = 1$. Am demonstrat deci că $f(x) = O(g(x))$. Reciproca nu este adevărată, adică din $f(x) = O(g(x))$ nu rezultă că $f(x) \sim g(x)$, deoarece $\lim_{x\to\infty} \frac{|f(x)|}{g(x)}$ s-ar putea să nu existe sau dacă există, s-ar putea ca $\lim_{x\to\infty} \frac{|f(x)|}{g(x)} \neq 1$. Dar aceasta contrazice că $f(x) \sim g(x)$, deoarece din $f(x) \sim g(x)$ rezultă că $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$ și deci rezultă, ca mai sus, că $\lim_{x\to\infty} \frac{|f(x)|}{g(x)} = 1$.

Exemplu.

$$x + \sin x \sim x,$$

deoarece dacă luăm $C_3 = 0$ atunci pentru orice x pentru care $x > C_3$ avem $x > 0$, iar $\lim_{x\to\infty} \frac{x+\sin x}{x} = \lim_{x\to\infty}\left(1 + \frac{\sin x}{x}\right) = 1$.

Cîteva proprietăți ale echivalenței asimptotice.

Ne referim numai la funcțiile pozitive în vecinătatea infinitului.

(1) *Relația definită mai sus este o relație de echivalență.*

Demonstrație. Sînt satisfăcute următoarele proprietăți.

(a) *reflexivitatea*: avem $f(x) \sim f(x)$, deoarece $\lim_{x\to\infty} \frac{f(x)}{f(x)} = 1$;

(b) *simetria*: dacă $f(x) \sim g(x)$ atunci $g(x) \sim f(x)$, deoarece dacă

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1 \text{ atunci } \lim_{x\to\infty} \frac{g(x)}{f(x)} = \lim_{x\to\infty} \frac{1}{\frac{f(x)}{g(x)}} = \frac{1}{\lim_{x\to\infty} \frac{f(x)}{g(x)}} = 1;$$

(c) *tranzitivitatea* : dacă $f(x)\sim g(x)$ și $g(x)\sim h(x)$ atunci $f(x)\sim h(x)$, deoarece dacă $\lim_{x\to\infty}\frac{f(x)}{g(x)}=1$, $\lim_{x\to\infty}\frac{g(x)}{h(x)}=1$, atunci $\lim_{x\to\infty}\frac{f(x)}{h(x)}=\lim_{x\to\infty}\frac{f(x)}{g(x)}\cdot\frac{g(x)}{h(x)}=\lim_{x\to\infty}\frac{f(x)}{g(x)}\lim_{x\to\infty}\frac{g(x)}{h(x)}=1$.

(2) *Dacă* $f(x)\sim g(x)$ *atunci* $f(x)=g(x)(1+o(1))$ *și reciproc.*

Demonstrație. Dacă $f(x)\sim g(x)$ atunci $\lim_{x\to\infty}\frac{f(x)}{g(x)}=1$. Deci $\lim_{x\to\infty}\frac{f(x)-g(x)}{g(x)}=\lim_{x\to\infty}\left(\frac{f(x)}{g(x)}-1\right)=\lim_{x\to\infty}\frac{f(x)}{g(x)}-1=0$, deci $\frac{f(x)-g(x)}{g(x)}=o(1)$, deci $f(x)=g(x)(1+o(1))$. Calculele putînd fi făcute în sens invers, înseamnă că reciproca este adevărată.

13.4. Evaluarea asimptotică a unor sume

Vom considera sume de forma

$$\sum_{v\leqslant n\leqslant x} f(n),$$

unde n parcurge toate numerele naturale diferite două cîte două cuprinse între două numere reale v și x, pentru care $v<x$, $f(u)$ fiind o funcție reală de variabilă reală u.

Teoremă. *Dacă funcția* $f(u)$ *este monotonă pe intervalul* $[v, +\infty)$ *și pozitivă pe intervalul* $(v, +\infty)$, *unde* v *este un număr întreg, atunci*

$$\sum_{v\leqslant n\leqslant x} f(n)=\int_v^x f(u)du+C+O(f(x)),$$

unde C *este o constantă nenegativă cînd funcția* $f(u)$ *este descrescătoare și este egală cu zero cînd funcția* $f(u)$ *este crescătoare, iar* $f(v)$ *este nenegativă.*

Demonstrație. Orice funcție monotonă pe intervalul $[v, x]$ este integrabilă pe acest interval, deci dacă funcția $f(u)$ este monotonă pe intervalul $[v, x]$ are sens să scriem

$$\int_v^x f(u)du.$$

Să luăm cazul cînd funcția $f(u)$ este descrescătoare pe intervalul $[v, +\infty)$. Rezultă că pentru orice u pentru care $n\leqslant u\leqslant n+1$, unde n este un număr întreg astfel încît $n\geqslant v$, avem

$$f(n)\geqslant f(u)\geqslant f(n+1).$$

Deci pentru numere întregi n pentru care $n\geqslant v$ avem

$$f(n)\geqslant\int_n^{n+1} f(u)du\geqslant f(n+1)$$

datorită proprietății de monotonie a integralei funcțiilor monotone, deoarece $f(n)=\int_n^{n+1} f(n)du$, același lucru fiind adevărat și pentru $f(n+1)$. Din inegalitățile

$$f(n)\geqslant\int_n^{n+1} f(u)du\geqslant f(n+1)$$

deducem

$$0\leqslant f(n)-\int_n^{n+1} f(u)du\leqslant f(n)-f(n+1),$$

deoarece din $f(n)\geqslant\int_n^{n+1} f(u)du$ rezultă $0\leqslant f(n)-\int_n^{n+1} f(u)du$, iar din $\int_n^{n+1} f(u)du\geqslant f(n+1)$ rezultă $-\int_n^{n+1} f(u)du\leqslant -f(n+1)$, deci $f(n)-\int_n^{n+1} f(u)du\leqslant f(n)-f(n+1)$.

Dacă notăm

$$A_n=f(n)-\int_n^{n+1} f(u)du$$

atunci pentru numerele întregi n din intervalul $[v, +\infty)$ se constată că avem

$$\sum_{y<n\leqslant z} A_n<f([y]+1),$$

deoarece dacă $y<n$, iar n este un număr întreg, atunci $[y]<n$, deci $[y]+1\leqslant n$ și deci

$$\sum_{y<n\leqslant z} A_n=\sum_{[y]+1\leqslant n\leqslant z} A_n\leqslant\sum_{[y]+1\leqslant n\leqslant z}(f(n)-f(n+1))=(f([y]+1)-f([y]+2))+$$

$$+(f([y]+2)-f([y]+3))+\ldots+(f([z])-f([z]+1))=$$

$$=f([y]+1)-f([z]+1)<f([y]+1).$$

Ultima evaluare s-a bazat pe faptul că funcţia $f(u)$ este pozitivă pe intervalul $(v, +\infty)$, deci $f([z]+1)>0$, deci $-f([z]+1)<0$, deci $f([y]+1)-f([z]+1)<f([y]+1)$.

Deci seria

$$\sum_{v\leqslant n} A_n$$

este convergentă, deoarece termenii acestei serii fiind nenegativi sumele parţiale ale acestei serii formează un şir crescător care este şi mărginit, datorită faptului că

$$\sum_{v\leqslant n\leqslant z} A_n<f(v)$$

conform calculului făcut mai sus, în care punem $v=[y]+1$. Vom nota cu C suma seriei pe care am pus-o în evidenţă adică

$$C=\sum_{v\leqslant n} A_n.$$

Avem deci

$$\sum_{v\leqslant n\leqslant x} f(n)-\int_v^x f(u)du-C=\sum_{v\leqslant n\leqslant x} f(n)-\sum_{v\leqslant n\leqslant [x]}\int_n^{n+1} f(u)du+\int_x^{[x]+1} f(u)du-$$

$$-\sum_{v\leqslant n} A_n=\sum_{v\leqslant n\leqslant x} f(n)-\sum_{v\leqslant n\leqslant x}\int_n^{n+1} f(u)du+\int_x^{[x]+1} f(u)du-\sum_{v\leqslant n} A_n=$$

$$=\sum_{v\leqslant n\leqslant x}\left(f(n)-\int_n^{n+1} f(u)du\right)+\int_x^{[x]+1} f(u)du-\sum_{v\leqslant n} A_n=-\sum_{x<n} A_n+\int_x^{[x]+1} f(u)du.$$

Avem $\sum_{[x]<n} A_n\leqslant f([x]+1)$, deoarece $\sum_{x<n} A_n=\lim_{z\to\infty}\sum_{x<n\leqslant z} A_n$, iar $\sum_{x\leqslant n\leqslant z} A_n<f([x]+1)$. Deci

$$\left|\sum_{v\leqslant n\leqslant x} f(n)-\int_v^x f(u)du-C\right|\leqslant\sum_{x<n} A_n+\int_x^{[x]+1} f(u)du\leqslant f([x]+1)+$$

$+f(x)\leqslant 2f(x)$, deoarece $\int_x^{[x]+1} f(u)du=u'([x]+1-x)\leqslant u'\leqslant f(x)$, unde $f(x)\geqslant u'\geqslant f([x]+1)$, datorită teoremei mediei pentru integrala unei funcţii monotone. Luînd constantele pozitive $C_1=3$ şi $C_2>$ $>\max(0, v)$ avem

$$f(x)>0 \text{ şi } \left|\sum_{v\leqslant n\leqslant x} f(n)-\int_v^x f(u)du-C\right|<C_1 f(x)$$

pentru orice x pentru care $x\geqslant C_2$, deci în acest caz teorema este demonstrată, constanta C fiind nenegativă.

Să luăm, acum, cazul cînd funcţia $f(u)$ este crescătoare pe intervalul $[v, +\infty)$. Aceasta înseamnă că pentru orice u, pentru care $n\leqslant u\leqslant n+1$, unde n este un număr întreg astfel încît $n\geqslant v$ avem

$$f(n)\leqslant f(u)\leqslant f(n+1).$$

Deci pentru numere întregi n pentru care $n\geqslant v$ avem

$$\int_n^{n+1} f(n)du\leqslant\int_n^{n+1} f(u)du\leqslant\int_n^{n+1} f(n+1)du$$

sau

$$f(n)\leqslant\int_n^{n+1} f(u)du\leqslant f(n+1)$$

datorită proprietăţii de monotonie a integralei funcţiilor monotone.

Din cauză că $\int_n^{n+1} f(u)du\leqslant f(n+1)$, avem $f(n+1)-\int_n^{n+1} f(u)du\geqslant 0$

deci

$$\sum_{v\leqslant n\leqslant x} f(n)-\int_v^x f(u)du=f(v)+\sum_{v\leqslant n\leqslant x-1} f(n+1)-\sum_{v\leqslant n\leqslant [x]-1}\int_n^{n+1} f(u)du-$$

$$-\int_{[x]}^x f(u)du=f(v)+\sum_{v\leqslant n\leqslant x-1} f(n+1)-\sum_{v\leqslant n\leqslant x-1}\int_n^{n+1} f(u)du-\int_{[x]}^x f(u)du=$$

$$=f(v)+\sum_{v\leqslant n\leqslant x-1}\left(f(n+1)-\int_n^{n+1} f(u)du\right)-\int_{[x]}^x f(u)du\geqslant-\int_{[x]}^x f(u)du,$$

$f(v)$ fiind nenegativă.

Însă $\int_{[x]}^x f(u)du=u'(x-[x])\leqslant u'\leqslant f(x)$, unde $f([x])\leqslant u'\leqslant f(x)$. Avem $u'(x-[x])\leqslant u'$ chiar dacă $x=[x]$, deoarece $u'\geqslant 0$ ca urmare a faptului că $0\leqslant f([x])$, funcţia $f(u)$ fiind pozitivă pe intervalul $(v, +\infty)$, iar $f(v)$ fiind nenegativă. Deci $-\int_{[x]}^x f(u)du\geqslant -f(x)$, deci

$$-f(x)\leqslant\sum_{v\leqslant n\leqslant x} f(n)-\int_v^x f(u)du.$$

Din cauză că $f(n) \leqslant \int_n^{n+1} f(u)du$, avem $f(n) - \int_n^{n+1} f(u)du \leqslant 0$ deci

$$\sum_{v \leqslant n \leqslant x} f(n) - \int_v^x f(u)du = \sum_{v \leqslant n \leqslant x-1} f(n) + f([x]) -$$

$$- \sum_{v \leqslant n \leqslant [x]-1} \int_n^{n+1} f(u)du - \int_{[x]}^x f(u)du = \sum_{v \leqslant n \leqslant x-1} (f(n) - \int_n^{n+1} f(u)du) +$$

$$+ f([x]) - \int_{[x]}^x f(u)du \leqslant f([x]) - \int_{[x]}^x f(u)du \leqslant f([x]) \leqslant f(x),$$

deoarece $\sum_{v \leqslant n \leqslant x-1} (f(n) - \int_n^{n+1} f(u)du) \leqslant 0$ și $\int_{[x]}^x f(u)du \geqslant 0$, funcția $f(u)$ fiind pozitivă pe intervalul $(v, +\infty)$. Deci

$$-f(x) \leqslant \sum_{v \leqslant n \leqslant x} f(n) - \int_v^x f(u)du \leqslant f(x),$$

deci

$$\left| \sum_{v \leqslant n \leqslant x} f(n) - \int_v^x f(u)du \right| \leqslant f(x).$$

Deci luînd constantele pozitive $C_1 = 2$ și $C_2 > \max(0, v)$ avem

$$f(x) > 0 \text{ și } \left| \sum_{v \leqslant n \leqslant x} f(n) - \int_v^x f(u)du \right| < C_1 f(x)$$

pentru orice x pentru care $x \geqslant C_2$, deci și în acest caz teorema este demonstrată.

Exemple.

(1) $\sum_{1 \leqslant n \leqslant x} \frac{1}{n} = \log x + C + O\left(\frac{1}{x}\right)$, *unde* C *este o constantă pozitivă.*

Demonstrație. Avem

$$\int_1^x \frac{du}{u} = \log x$$

și aplicăm teorema demonstrată, funcția $f(u) = \frac{1}{u}$ fiind descrescătoare pe intervalul $[1, +\infty)$, deoarece pe acest interval $f'(u) = -\frac{1}{u^2} < 0$, funcția $f(u) = \frac{1}{u}$ fiind și pozitivă pe intervalul $(1, +\infty)$. Constanta C este pozitivă, deoarece în $C = \sum_{1 \leqslant n} A_n$ avem

$$A_1 = \frac{1}{1} - \int_1^2 \frac{1}{u} du = 1 - \log 2 = \log \frac{e}{2} > 0,$$

e fiind baza logaritmilor naturali.

(2) *Dacă* $\rho \neq 0$ *atunci*

$$\sum_{1 \leqslant n \leqslant x} n^{-1-\rho} = -\rho^{-1} x^{-\rho} + K + O(x^{-1-\rho}),$$

unde K *este o constantă, care este egală cu* 0 *dacă* $\rho \leqslant -1$.

Demonstrație. Avem

$$\int_1^x u^{-1-\rho} du = \left. \frac{u^{-\rho}}{-\rho} \right|_1^x = -\rho^{-1} x^{-\rho} + \frac{1}{\rho}$$

și după aplicarea teoremei de mai sus luăm $K = C + \frac{1}{\rho}$. Putem aplica teorema de mai sus, deoarece aici intervine funcția $f(u) = u^{-1-\rho}$. Această funcție este pozitivă pe intervalul $(1, +\infty)$. Apoi $f'(u) = (-1-\rho)u^{-2-\rho}$. Pe intervalul $[1, +\infty)$ această funcție este descrescătoare dacă $1 + \rho \geqslant 0$, adică dacă $\rho \geqslant -1$. Pe același interval $[1, +\infty)$ funcția considerată este crescătoare dacă $1 + \rho \leqslant 0$, adică daeă $\rho \leqslant -1$, iar $f(1)$ este nenegativă, deoarece $f(1) = 1$. În acest caz $C = 0$, iar $K = \frac{1}{\rho}$. Dar avem $K = O(x^{-1-\rho})$, deoarece luînd $C_3 = 0$, pentru orice x pentru care $x \geqslant C_3$ avem $x^{-1-\rho} > 0$, iar $\lim_{x \to \infty} \frac{K}{x^{-1-\rho}} = 0$ atunci cînd $1 + \rho \leqslant 0$. Putem deci să-l înglobăm pe K în termenul $O(x^{-1-\rho})$ atunci cînd $\rho \leqslant -1$, deoarece $O(x^{-1-\rho}) + O(x^{-1-\rho}) = O(x^{-1-\rho})$.

(3) $\sum_{1 \leqslant n \leqslant x} \log n = x \log x - x + O(\log x)$.

Demonstrație. Funcția $f(u)=\log u$ este crescătoare pe intervalul $[1, +\infty)$, deoarece $f'(u)=\frac{1}{u}>0$, pe acest interval și este pozitivă pe intervalul $(1, +\infty)$, iar $f(1)$ este nenegativă, pentru că $f(1)=0$. De aceea în teorema de mai sus avem $C=0$. Apoi

$$\int_1^x \log u\,du = u\log u\Big|_1^x - \int_1^x du = x\log x - x + 1.$$

Mai avem $1=O(\log x)$, deci relația de mai sus este demonstrată.

(4) $$\sum_{1\leqslant n\leqslant x}\frac{\log n}{n}=\frac{1}{2}\log^2 x+K+O\left(\frac{\log x}{x}\right),$$ *unde K este o constantă.*

Demonstrație. Avem $f'(u)=\frac{1-\log u}{u^2}$, unde $f(u)=\frac{\log u}{u}$. Deci funcția $f(u)$ este descrescătoare pentru $u>e$, deoarece pentru aceste valori ale lui u avem $f'(u)=\frac{\log\frac{e}{u}}{u^2}<0$. Obținem

$$\sum_{3\leqslant n\leqslant x}\frac{\log n}{n}=\int_3^x\frac{\log u}{u}du+C+O\left(\frac{\log x}{x}\right)=\frac{1}{2}\log^2 u\Big|_3^x+C+$$

$$+O\left(\frac{\log x}{x}\right)=\frac{1}{2}\log^2 x+\left(C-\frac{1}{2}\log^2 3\right)+O\left(\frac{\log x}{x}\right),$$

unde C este o constantă nenegativă, deoarece $f(u)$, unde $f(u)=\frac{\log u}{u}$, este descrescătoare pe intervalul $[3, +\infty)$ și pozitivă pe intervalul $(3, +\infty)$. Căpătăm

$$\sum_{1\leqslant n\leqslant x}\frac{\log n}{n}=\frac{1}{2}\log^2 x+K+O\left(\frac{\log x}{x}\right),$$

unde K este o constantă, deoarece $K=C+\frac{\log 2}{2}-\frac{1}{2}\log^2 3$.

(5) $$\sum_{2\leqslant n\leqslant x}\frac{1}{n\log n}=\log\log x+K+O\left(\frac{1}{x\log x}\right),$$

unde K este o constantă.

Demonstrație. Funcția $f(u)=\frac{1}{u\log u}$ este descrescătoare pe intervalul $[2, +\infty)$, deoarece $f'(u)=\frac{-\log u-1}{(u\log u)^2}<0$, pentru $u\geqslant 2$ și este pozitivă pe intervalul $(2, +\infty)$. Apoi

$$\int_2^x\frac{du}{u\log u}=\log\log u\Big|_2^x=\log\log x-\log\log 2,$$

deci, conform teoremei de mai sus, avem $K=C-\log\log 2$, unde C este o constantă nenegativă.

(6) $$\sum_{2\leqslant n\leqslant x}\frac{1}{n\log^2 n}=-\frac{1}{\log x}+K+O\left(\frac{1}{x\log^2 x}\right),$$

unde K este o constantă pozitivă.

Demonstrație. Funcția $f(u)=\frac{1}{u\log^2 u}$ este descrescătoare pe intervalul $[2, +\infty)$, deoarece $f'(u)=\frac{-\log^2 u-2\log u}{(u\log^2 u)^2}<0$ pentru $u\geqslant 2$ și este pozitivă pe intervalul $(2, +\infty)$. Apoi

$$\int_2^x\frac{du}{u\log^2 u}=-\frac{1}{\log u}\Big|_2^x=-\frac{1}{\log x}+\frac{1}{\log 2},$$

deci, conform teoremei de mai sus, avem $K=C+\frac{1}{\log 2}$ care este o constantă pozitivă.

(7) $$\sum_{2\leqslant n\leqslant x}\frac{1}{\log n}=o(x).$$

Demonstrație. Funcția $f(u)=\frac{1}{\log u}$ este descrescătoare pe inter-

valul $[2, +\infty)$, deoarece $f'(u)=-\frac{1}{u\log^2 u}<0$ pentru $u\geqslant 2$, și este pozitivă pe intervalul $(2, +\infty)$. Apoi

$$\int_2^x \frac{du}{\log u}=\frac{u}{\log u}\Big|_2^x-\int_2^x \frac{u\,du}{-u\log^2 u}=\frac{x}{\log x}-\frac{2}{\log 2}+\int_2^{\sqrt{x}}\frac{du}{\log^2 u}+\int_{\sqrt{x}}^x \frac{du}{\log^2 u}\leqslant$$

$$\leqslant \frac{x}{\log x}-\frac{2}{\log 2}+\frac{\sqrt{x}-2}{\log^2 2}+\frac{x-\sqrt{x}}{\log^2\sqrt{x}}=\frac{x}{\log x}-\frac{2}{\log 2}+\frac{\sqrt{x}}{\log^2 2}-\frac{2}{\log^2 2}+$$

$$+\frac{x-\sqrt{x}}{\log^2\sqrt{x}}=\frac{x}{\log x}+O\left(\frac{x}{\log^2 x}\right)=o(x).$$

Avînd în vedere că

$$\sum_{2\leqslant n\leqslant x}\frac{1}{\log n}=\int_2^x\frac{du}{\log u}+C+O\left(\frac{1}{\log x}\right),$$

deducem enunțul proprietății, deoarece $C=o(x)$, $O\left(\frac{1}{\log x}\right)=o(x)$.

Consecințe.

(1) *Dacă* $\rho>0$, *atunci*

$$\sum_{1\leqslant n\leqslant x} n^{-1-\rho}=O(1).$$

Într-adevăr,

$$\sum_{1\leqslant n\leqslant x} n^{-1-\rho}=-\rho^{-1}x^{-\rho}+K+O(x^{-1-\rho}).$$

Dacă $\rho>0$, avem

$$|-\rho^{-1}x^{-\rho}|=\left|\frac{1}{\rho}\right|\left|\frac{1}{x^\rho}\right|<\frac{1}{\rho}$$

pentru $x>1$. Deci dacă luăm constantele pozitive $C_1=\frac{1}{\rho}$ și $C_2=1$, avem

$$|-\rho^{-1}x^{-\rho}|<C_1\cdot 1$$

pentru orice x pentru care $x>C_2$. Deci dacă $\rho>0$ avem $-\rho^{-1}x^{-\rho}=$

$=O(1)$. Apoi $K=O(1)$, deoarece K este o funcție mărginită în vecinătatea infinitului. În fine, dacă $\rho>0$ avem

$$|x^{-1-\rho}|=\left|\frac{1}{x^{1+\rho}}\right|<1,$$

pentru $x>1$. Deci luînd constantele pozitive $C_1=1$ și $C_2=1$, avem

$$|x^{-1-\rho}|<C_1\cdot 1,$$

pentru orice x pentru care $x>C_2$, deci $x^{-1-\rho}=O(1)$. Rezultă că dacă $\rho>0$, atunci

$$\sum_{1\leqslant n\leqslant x} n^{-1-\rho}=O(1)+O(1)+O(O(1))=O(1).$$

În evaluările de mai sus am ținut seama de faptul că dacă $\mu>0$ atunci

$$x^\mu>1, \text{ pentru } x>1.$$

Aceasta se demonstrează în felul următor. Se consideră funcția

$$f(x)=x^\mu-1.$$

Avem $f'(x)=\mu x^{\mu-1}>0$, pentru $x>1$, deci pentru $x>1$ funcția considerată este crescătoare. Rezultă că $f(x)>f(1)$ pentru $x>1$ și deoarece $f(1)=0$ obținem $x^\mu-1>0$, de unde $x^\mu>1$ pentru $x>1$.

(2) *Dacă* $t\geqslant 1{,}5$ *atunci*

$$\sum_{1\leqslant n\leqslant x} n^{-t}\log^k n=O(1),$$

unde k *este un număr real.*

Într-adevăr, am demonstrat că $\log^\alpha x=o(x^\beta)$, unde α și β sînt numere reale cu $\beta>0$. Aceasta înseamnă că $\lim\limits_{x\to\infty}\frac{\log^\alpha x}{x^\beta}=0$, deci pentru orice număr real pozitiv ε există un număr real C astfel încît

$$\left|\frac{\log^\alpha x}{x^\beta}-0\right|<\varepsilon$$

pentru orice x pentru care $x>C$. Așadar

$$-\varepsilon<\frac{\log^\alpha x}{x^\beta}<\varepsilon$$

pentru orice x pentru care $x>C$, deci există un număr real C astfel încît

$$\log^{\alpha} x<x^{\beta}$$

pentru orice x pentru care $x>C$, deoarece putem lua $\varepsilon=1$. Dacă n este un număr natural cu $n>C$, atunci

$$\log^{k} n<n^{\frac{1}{4}}.$$

Aşadar

$$\left|\sum_{1\leqslant n\leqslant x} n^{-t}\log^{k} n\right|=\sum_{1\leqslant n\leqslant C} n^{-t}\log^{k} n+\sum_{C<n\leqslant x} n^{-t}\log^{k} n<$$

$$<\sum_{1\leqslant n\leqslant C} n^{-t}\log^{k} n+\sum_{C<n\leqslant x} n^{-t}\,n^{1/4}=\sum_{1\leqslant n\leqslant C} n^{-t}\log^{k} n-$$

$$-\sum_{1\leqslant n\leqslant C} n^{-t+0,25}+\sum_{1\leqslant n\leqslant x} n^{-t+0,25}=O(1)+O(1)+O(1)=O(1)$$

ultima sumă fiind $O(1)$, deoarece $-t+0{,}25\leqslant -1{,}25$ şi folosim consecinţa (1). Primele două sume sînt $O(1)$, deoarece sînt constante. Din cauză că

$$\left|\sum_{1\leqslant n\leqslant x} n^{-t}\log^{k} n\right|<O(1),$$

deducem că $\sum_{1\leqslant n\leqslant x} n^{-t}\log^{k} n=O(1)$, pentru $t\geqslant 1{,}5$.

Capitolul 14

EVALUĂRI ASIMPTOTICE ALE CÎTORVA FUNCŢII NUMERICE

14.1. Evaluarea asimptotică a funcţiei $\Psi(x)$

Teoremă. $\Psi(x)=O(x)$.

Demonstraţie. Avem $\Psi(x)=\sum_{1\leqslant n\leqslant x}\Lambda(n)=$

$$=\sum_{1\leqslant n\leqslant x}\sum_{d\mid n}\mu(d)\log\frac{n}{d}=\sum_{1\leqslant n\leqslant x}\sum_{d\mid n}\mu(d)(\log n-\log d)=$$

$$=\sum_{1\leqslant n\leqslant x}\left(\sum_{d\mid n}\mu(d)\right)\log n-\sum_{1\leqslant n\leqslant x}\sum_{d\mid n}\mu(d)\log d=$$

$$=-\sum_{1\leqslant n\leqslant x}\sum_{d\mid n}\mu(d)\log d=\sum_{1\leqslant n\leqslant x}\left(\sum_{d\mid n}\mu(d)\right)\log x-\log x-$$

$$-\sum_{1\leqslant n\leqslant x}\sum_{d\mid n}\mu(d)\log d=\sum_{1\leqslant n\leqslant x}\sum_{d\mid n}\mu(d)(\log x-\log d)-\log x=$$

$$= \sum_{1\leqslant n\leqslant x} \sum_{d\mid n} \mu(d)\ \log\frac{x}{d} - \log\ x = \sum_{1\leqslant d\leqslant x} \sum_{1\leqslant t\leqslant \frac{x}{d}} \mu(d)\ \log\frac{x}{d} - \log\ x =$$

$$= \sum_{1\leqslant d\leqslant x} \left[\frac{x}{d}\right] \mu(d)\ \log\frac{x}{d} - \log\ x = x \sum_{1\leqslant d\leqslant x} \frac{\mu(d)}{d} \log\frac{x}{d} -$$

$$- \sum_{1\leqslant d\leqslant x} \left\{\frac{x}{d}\right\} \mu(d) \log\frac{x}{d} - \log\ x.$$

Avem

$$\sum_{1\leqslant d\leqslant x} \frac{\mu(d)}{d} \log\frac{x}{d} = \sum_{1\leqslant d\leqslant x} \frac{\mu(d)}{d} \left(\sum_{1\leqslant n\leqslant \frac{x}{d}} \frac{1}{n} - C - O\left(\frac{1}{\frac{x}{d}}\right)\right) =$$

$$= \sum_{1\leqslant d\leqslant x} \sum_{1\leqslant n\leqslant \frac{x}{d}} \frac{\mu(d)}{nd} - C \sum_{1\leqslant d\leqslant x} \frac{\mu(d)}{d} - \sum_{1\leqslant d\leqslant x} \frac{\mu(d)}{d} O\left(\frac{d}{x}\right).$$

Însă

$$\sum_{1\leqslant d\leqslant x} \sum_{1\leqslant n\leqslant \frac{x}{d}} \frac{\mu(d)}{nd} = \sum_{1\leqslant c\leqslant x} \sum_{d\mid c} \frac{\mu(d)}{c} = \sum_{1\leqslant c\leqslant x} \frac{1}{c} \sum_{d\mid c} \mu(d) = 1 = O(1).$$

Apoi

$$1 = \sum_{1\leqslant n\leqslant x} \sum_{d\mid n} \mu(d) = \sum_{1\leqslant d\leqslant x} \sum_{1\leqslant t\leqslant \frac{x}{d}} \mu(d) = \sum_{1\leqslant d\leqslant x} \left[\frac{x}{d}\right] \mu(d) =$$

$$= x \sum_{1\leqslant d\leqslant x} \frac{\mu(d)}{d} - \sum_{1\leqslant d\leqslant x} \left\{\frac{x}{d}\right\} \mu(d).$$

Deci

$$\left| x \sum_{1\leqslant d\leqslant x} \frac{\mu(d)}{d} \right| = \left| 1 + \sum_{1\leqslant d\leqslant x} \left\{\frac{x}{d}\right\} \mu(d) \right| = \left| 1 + \left\{\frac{x}{1}\right\} + \right.$$

$$\left. + \sum_{2\leqslant d\leqslant x} \left\{\frac{x}{d}\right\} \mu(d) \right| \leqslant 1 + \{x\} + \sum_{2\leqslant d\leqslant x} \left\{\frac{x}{d}\right\} \leqslant 1 + \{x\} + [x] - 1 = x.$$

Aşadar $\left| \sum_{1\leqslant d\leqslant x} \frac{\mu(d)}{d} \right| \leqslant 1 = O(1)$, deci $\sum_{1\leqslant d\leqslant x} \frac{\mu(d)}{d} = O(1)$.

În fine,

$$\left| \sum_{1\leqslant d\leqslant x} \frac{\mu(d)}{d} O\left(\frac{d}{x}\right) \right| \leqslant \sum_{1\leqslant d\leqslant x} \left| \frac{\mu(d)}{d} \right| \left| O\left(\frac{d}{x}\right) \right| \leqslant \sum_{1\leqslant d\leqslant x} \frac{1}{d} O\left(\frac{d}{x}\right) =$$

$$= O\left(\sum_{1\leqslant d\leqslant x} \left| \frac{1}{d} \right| \left| \frac{d}{x} \right| \right) = O\left(\frac{[x]}{x}\right) = O(O(1)) = O(1).$$

Obţinem, deci

$$\sum_{1\leqslant d\leqslant x} \frac{\mu(d)}{d} O\left(\frac{d}{x}\right) = O(1).$$

Am putut scrie

$$\sum_{1\leqslant d\leqslant x} \frac{1}{d} O\left(\frac{d}{x}\right) = O\left(\sum_{1\leqslant d\leqslant x} \left| \frac{1}{d} \right| \left| \frac{d}{x} \right| \right),$$

deoarece notînd $f(x) = \frac{1}{x}$, $h(x) = O\left(\frac{1}{x}\right)$, $g(x) = \frac{1}{x}$, se constată că $f(x)$ este definită pentru orice număr natural x, iar $h(x)$ şi $g(x)$ sînt definite pentru orice x pentru care $x \geqslant 1$. Funcţia $h(x)$ este mărginită pe intervalul $[1, \alpha]$ pentru orice α pentru care $\alpha \geqslant 1$, deoarece avem

$$h(x) = \sum_{1\leqslant n\leqslant x} \frac{1}{n} - C - \log\ x.$$

Apoi se vede că $|g(x)| \geqslant \frac{1}{\alpha}$ pentru orice x pentru care $\alpha \geqslant x \geqslant 1$, iar dacă luăm $a = 1$ rezultă că $f(a) \neq 0$. Deci se aplică teorema care spune că în condiţiile de mai sus avem

$$\sum_{1\leqslant n\leqslant x} f(n) h\left(\frac{x}{n}\right) = O\left(\sum_{1\leqslant n\leqslant x} \left| f(n) \right| \left| g\left(\frac{x}{n}\right) \right| \right).$$

Am demonstrat, deci că

$$\sum_{1\leqslant d\leqslant x} \frac{\mu(d)}{d} \log\frac{x}{d} = O(1).$$

Mai avem

$$\left|\sum_{1\leqslant d\leqslant x}\left\{\frac{x}{d}\right\}\mu(d)\log\frac{x}{d}\right|\leqslant\sum_{1\leqslant d\leqslant x}\log\frac{x}{d}=\sum_{1\leqslant d\leqslant x}(\log x-\log d)=$$

$$=\sum_{1\leqslant d\leqslant x}\log x-\sum_{1\leqslant d\leqslant x}\log d=[x]\log x-(x\log x-x+O(\log x))=$$

$$=-\{x\}\log x+x-O(\log x)=O(x),$$

deci

$$\sum_{1\leqslant d\leqslant x}\left\{\frac{x}{d}\right\}\mu(d)\log\frac{x}{d}=O(x).$$

Aşadar,

$$\Psi(x)=xO(1)-\log x-O(x)=O(x).$$

14.2. Evaluări asimptotice ale unor sume în care intervine funcţia lui Mangoldt

$$(1)\quad\sum_{1\leqslant n\leqslant x}\frac{\Lambda(n)}{n}=\log x+O(1).$$

Demonstraţie. Avem

$$\sum_{1\leqslant n\leqslant x}\log n=\sum_{1\leqslant n\leqslant x}\sum_{d\mid n}\Lambda(d)=\sum_{1\leqslant d\leqslant x}\sum_{1\leqslant t\leqslant\frac{x}{d}}\Lambda(d)=$$

$$=\sum_{1\leqslant d\leqslant x}\left[\frac{x}{d}\right]\Lambda(d)=x\sum_{1\leqslant d\leqslant x}\frac{\Lambda(d)}{d}-\sum_{1\leqslant d\leqslant x}\left\{\frac{x}{d}\right\}\Lambda(d).$$

Deci

$$\sum_{1\leqslant d\leqslant x}\frac{\Lambda(d)}{d}=\frac{1}{x}\sum_{1\leqslant n\leqslant x}\log n+\frac{1}{x}\sum_{1\leqslant d\leqslant x}\left\{\frac{x}{d}\right\}\Lambda(d)=$$

$$=\frac{1}{x}(x\log x-x+O(\log x))+\frac{1}{x}\sum_{1\leqslant d\leqslant x}\left\{\frac{x}{d}\right\}\Lambda(d)=\log x-1+$$

$$+O\left(\frac{\log x}{x}\right)+\frac{1}{x}\sum_{1\leqslant d\leqslant x}\left\{\frac{x}{d}\right\}\Lambda(d).$$

Dar luînd o constantă $C_3=0$, avem $x>0$ pentru orice x pentru care $x>C_3$ şi $\lim\limits_{x\to\infty}\frac{\log x}{x}=0$ deci $\frac{\log x}{x}=O(1)$ şi apoi

$$\left|\frac{1}{x}\sum_{1\leqslant d\leqslant x}\left\{\frac{x}{d}\right\}\Lambda(d)\right|\leqslant\frac{1}{x}\sum_{1\leqslant d\leqslant x}\Lambda(d)=\frac{1}{x}\Psi(x)=O\left(\frac{x}{x}\right)=O(1).$$

Obţinem

$$\sum_{1\leqslant d\leqslant x}\frac{\Lambda(d)}{d}=\log x-1+O(O(1))+O(1)=\log x+O(1).$$

Înainte de a evalua alte sume, vom stabili formula de transformare a sumelor datorată lui Abel.

Teoremă. *Fiind date două şiruri de numere* $a_1, a_2, \ldots, b_1, b_2, \ldots$ *avem*

$$\sum_{i=m}^{n}a_ib_i=\sum_{k=m}^{n}s_k(b_k-b_{k+1})+b_{n+1}s_n,$$

unde $s_j=\sum\limits_{l=m}^{j}a_l$.

Demonstraţie. Avem $a_i=s_i-s_{i-1}$ pentru $i\geqslant m$, dacă punem $s_{m-1}=0$. Deci

$$\sum_{i=m}^{n}a_ib_i=\sum_{i=m}^{n}(s_i-s_{i-1})b_i=\sum_{i=m}^{n}s_ib_i-\sum_{i=m}^{n}s_{i-1}b_i=$$

$$=\sum_{i=m}^{n}s_ib_i-\sum_{i=m}^{n-1}s_ib_{i+1}=\sum_{i=m}^{n}s_ib_i-\sum_{i=m}^{n}s_ib_{i+1}+s_nb_{n+1}=$$

$$= \sum_{k=m}^{n} s_k(b_k - b_{k+1}) + b_{n+1}s_n.$$

(2) $$\sum_{1\leqslant n\leqslant x} \frac{\Lambda(n)}{n} \log\ n = \frac{1}{2}\log^2 x + O(\log\ x).$$

Demonstrație. Scriind

$$\sum_{1\leqslant n\leqslant x} \frac{\Lambda(n)}{n} \log\ n = \sum_{i=1}^{[x]} a_i b_i,$$

unde $a_i = \frac{\Lambda(i)}{i}$, $b_i = \log i$, putem aplica formula de transformare a sumelor a lui Abel, obținînd

$$\sum_{1\leqslant n\leqslant x} \frac{\Lambda(n)}{n} \log\ n = \sum_{k=1}^{[x]} \left(\sum_{i=1}^{k} \frac{\Lambda(i)}{i}\right)(\log\ k - \log(k+1)) +$$

$$+ \sum_{i=1}^{[x]} \frac{\Lambda(i)}{i} \log([x]+1) = \sum_{1\leqslant k\leqslant x} \left(\sum_{1\leqslant i\leqslant k} \frac{\Lambda(i)}{i}\right)(\log\ k - \log\ (k+1)) +$$

$$+ \left(\sum_{1\leqslant i\leqslant x} \frac{\Lambda(i)}{i}\right)\log([x]+1).$$

Ținînd seama de faptul că

$$\log\ (x+h) = \log x + \frac{h}{x} + O\left(\frac{1}{x^2}\right),$$

unde h este o constantă obținem

$$\log(k+1) = \log\ k + \frac{1}{k} + O\ \frac{1}{k^2}\Big).$$

Apoi

$$\left|\log([x]+1) - \log\ x\right| = \left|\log\left(\frac{x}{[x]+1}\right)\right| = \left|O\left(\frac{x}{[x]+1}\right)\right| = O(O(1)) = O(1)$$

deci $\log\ ([x]+1) = \log\ x + O(1)$.

Așadar,

$$\sum_{1\leqslant n\leqslant x} \frac{\Lambda(n)}{n} \log\ n = \sum_{1\leqslant k\leqslant x} (\log\ k + O(1))\left(-\frac{1}{k} - O\left(\frac{1}{k^2}\right)\right) +$$

$$+ (\log\ x + O(1))(\log\ x + O(1)) = -\sum_{1\leqslant k\leqslant x} \frac{\log\ k}{k} - \sum_{1\leqslant k\leqslant x} \left(\frac{1}{k} O(1) + \right.$$

$$\left. + O\left(\frac{1}{k^2}\right)\log\ k + O(1)O\left(\frac{1}{k^2}\right)\right) + (\log\ x + O(1))(\log\ x + O(1)) =$$

$$= -\left(\frac{1}{2}\log^2 x + K + O\left(\frac{\log\ x}{x}\right)\right) - \sum_{1\leqslant k\leqslant x} O\left(\frac{1}{k}\right) + \log^2 x + \log\ x\ O(1) +$$

$$+ \log x\ O(1) + O(1)O(1) = \frac{1}{2}\log^2\ x - K - O\left(\frac{\log\ x}{x}\right) - O\left(\sum_{1\leqslant k\leqslant x} \frac{1}{k}\right) +$$

$$+ O(\log\ x),$$

deoarece

$$\frac{1}{k} O(1) + O\left(\frac{1}{k^2}\right)\log\ k + O(1)O\left(\frac{1}{k^2}\right) = O\left(\frac{1}{k}\right) + O\left(\frac{\log\ k}{k^2}\right) +$$

$$+ O\left(O\left(\frac{1}{k^2}\right)\right) = O\left(\frac{1}{k}\right) + O\left(O\left(\frac{1}{k}\right)\right) + O\left(O\left(O\left(\frac{1}{k}\right)\right)\right) = O\left(\frac{1}{k}\right),$$

iar $O(1) = O(\log\ x)$.

Am putut scrie $O(1)O\left(\frac{1}{k^2}\right) = O\left(O\left(\frac{1}{k^2}\right)\right)$, deoarece $O\left(\frac{1}{k^2}\right) = \log(k+1) - \log\ k - \frac{1}{k}$, iar pentru funcția $k(x) = \log(x+1) - \log\ x - \frac{1}{x}$ există o constantă x_k astfel încît $k(x) \neq 0$ pentru orice x pentru care $x > x_k$. Într-adevăr, avem $k'(x) = \frac{1}{x+1} - \frac{1}{x} + \frac{1}{x^2} = \frac{1}{(x+1)x^2} > 0$ pentru orice x pentru care $x > 0$. Deci funcția $k(x)$ este crescătoare pentru orice x pentru care $x > 0$. Apoi $\lim\limits_{x\to\infty} k(x) = 0$ deci $k(x) < 0$ pentru orice x pentru care $x > 0$, funcția $k(x)$ fiind și continuă pentru orice x pentru care $x > 0$. Deci dacă luăm $x_k = 0$, avem $k(x) \neq 0$ pentru orice x pentru care $x > x_k$.

Am mai putut scrie $O(1)O(1)=O(O(1))=O(1)$, deoarece cu $O(1)$ provenit din $\log([x]+1)=\log x+O(1)$ avem $\log([x]+1)-\log x=$ $=\log\left(\frac{[x]+1}{x}\right)>0$ pentru orice x pentru care $x>0$. Deci luînd $k(x)=\log([x]+1)-\log x$ și $x_k=0$ avem $k(x)\neq 0$ pentru orice x pentru care $x>x_k$.

Funcția $h(x)=\frac{1}{x}O(1)+O\left(\frac{1}{x^2}\right)\log x+O(1)O\left(\frac{1}{x^2}\right)=O\left(\frac{1}{x}\right)$ este definită pentru orice număr natural x, deoarece $\frac{1}{x}$, $\log x$ sînt definite pentru orice număr natural x, iar funcțiile $O(1)$, $O\left(\frac{1}{x^2}\right)$ sînt definite pentru orice număr natural x, ele provenind din formulele

$$\sum_{1\leqslant n\leqslant x}\frac{\Lambda(n)}{n}=\log x+O(1),\quad \log(x+1)=\log x+\frac{1}{x}+O\left(\frac{1}{x^2}\right).$$

Deoarece și funcțiile $f(x)=1$, $g(x)=\frac{1}{x}$ sînt definite pentru orice număr natural x, putem aplica teorema care spune că

$$\sum_{1\leqslant n\leqslant x}f(n)h(n)=O\left(\sum_{1\leqslant n\leqslant x}|f(n)||g(n)|\right),$$

deoarece mai avem că $f(a)g(a)=\frac{1}{a}\neq 0$ pentru orice număr natura a, deci există un număr natural a astfel încît $f(a)g(a)\neq 0$. Din această cauză am scris

$$\sum_{1\leqslant k\leqslant x}O\left(\frac{1}{k}\right)=O\left(\sum_{1\leqslant k\leqslant x}\frac{1}{k}\right).$$

Însă

$$O\left(\sum_{1\leqslant k\leqslant x}\frac{1}{k}\right)=O\left(\log x+C+O\left(\frac{1}{x}\right)\right)=O(O(\log x))=O(\log x)$$

și cum mai avem $K=O(\log x)$, $\frac{\log x}{x}=O(\log x)$, rezultă că proprietatea (2) este demonstrată.

(3) $$\sum_{mn\leqslant x}\frac{\Lambda(m)\,\Lambda(n)}{mn}=\frac{1}{2}\log^2 x+O(\log x),$$

unde suma $\sum_{mn\leqslant x}\frac{\Lambda(m)\,\Lambda(n)}{mn}$ *se face pentru toate perechile de numere naturale* (m, n) *pentru care produsul* mn *este cel mult egal cu un număr real* x, *fiecare pereche* (m, n) *fiind luată o singură dată.*

Demonstrație. Avem

$$\sum_{mn\leqslant x}\frac{\Lambda(m)\,\Lambda(n)}{mn}=\sum_{1\leqslant n\leqslant x}\sum_{1\leqslant m\leqslant\frac{x}{n}}\frac{\Lambda(m)\,\Lambda(n)}{mn}=$$

$$=\sum_{1\leqslant n\leqslant x}\frac{\Lambda(n)}{n}\left(\sum_{1\leqslant m\leqslant\frac{x}{n}}\frac{\Lambda(m)}{m}\right)=\sum_{1\leqslant n\leqslant x}\frac{\Lambda(n)}{n}\left(\log\frac{x}{n}+O(1)\right)=$$

$$=\left(\sum_{1\leqslant n\leqslant x}\frac{\Lambda(n)}{n}\right)\log x-\sum_{1\leqslant n\leqslant x}\frac{\Lambda(n)}{n}\log n+\sum_{1\leqslant n\leqslant x}\frac{\Lambda(n)}{n}O(1)=$$

$$=(\log x+O(1))\log x-\left(\frac{1}{2}\log^2 x+O(\log x)\right)+O\left(\sum_{1\leqslant n\leqslant x}\frac{\Lambda(n)}{n}\right).$$

Am transformat ultima sumă în $O\left(\sum_{1\leqslant n\leqslant x}\frac{\Lambda(n)}{n}\right)$, deoarece funcția $f(x)=\frac{\Lambda(x)}{x}$ este definită pentru orice număr natural x, funcțiile $g(x)=1$, $h(x)=O(1)=\sum_{1\leqslant n\leqslant x}\frac{\Lambda(n)}{n}-\log x$ sînt definite pentru orice x pentru care $x\geqslant 1$, $|g(x)|\geqslant 1$ pentru orice x pentru care $x\geqslant 1$ și există un număr natural a, de exemplu 2, pentru care $f(a)\neq 0$, avînd în vedere că $f(2)=\frac{\Lambda(2)}{2}=\frac{\log 2}{2}$. Funcția $h(x)$ este și mărginită pe intervalul $[1, \alpha]$ pentru orice α pentru care $\alpha\geqslant 1$. Am putut deci utiliza relația

$$\sum_{1\leqslant n\leqslant x}f(n)h\left(\frac{x}{n}\right)=O\left(\sum_{1\leqslant n\leqslant x}\left|f(n)\right|\left|g\left(\frac{x}{n}\right)\right|\right)$$

în care $f(n)=\frac{\Lambda(n)}{n}$, $h\left(\frac{x}{n}\right)=O(1)$, $g\left(\frac{x}{n}\right)=1$.

Deci

$$\sum_{mn\leqslant x}\frac{\Lambda(m)\ \Lambda(n)}{mn}=\frac{1}{2}\log^2 x+O(1)\log x-O(\log x)+O(\log x+$$

$$+O(1))=\frac{1}{2}\log^2 x+O(\log x).$$

$$(4)\quad \sum_{mn\leqslant x}\frac{\Lambda(m)\ \Lambda(n)}{mn\ \log mn}=\log x+O(\log\log x),$$

unde suma $\sum_{mn\leqslant x}\frac{\Lambda(m)\ \Lambda(n)}{mn\log mn}$ *se face pentru toate perechile de numere naturale* (m, n) *pentru care produsul* mn *este cel mult egal cu un număr real* x, *fiecare pereche* (m, n) *fiind luată o singură dată. Termenul* $\frac{\Lambda(1)\Lambda(1)}{1\cdot 1\log 1\cdot 1}$ *care nu are sens, avînd forma* $\frac{0}{0}$, *se presupune că este înlocuit cu* 0.

Demonstrație. Avem

$$\sum_{mn\leqslant x}\frac{\Lambda(m)\ \Lambda(n)}{mn\ \log\ mn}=\sum_{1\leqslant m\leqslant x}\ \sum_{1\leqslant n\leqslant\frac{x}{m}}\frac{\Lambda(m)\ \Lambda(n)}{mn\log\ mn}=$$

$$=\sum_{1\leqslant c\leqslant x}\ \sum_{n|c}\frac{\Lambda(n)\ \Lambda\left(\frac{c}{n}\right)}{c\ \log\ c}=\sum_{2\leqslant c\leqslant x}\ \sum_{n|c}\frac{\Lambda(n)\ \Lambda\left(\frac{c}{n}\right)}{c\ \log\ c},$$

deoarece termenul $\frac{\Lambda(1)\,\Lambda\left(\frac{1}{1}\right)}{1\ \log\ 1}$, care este identic cu termenul $\frac{\Lambda(1)\ \Lambda(1)}{1\cdot 1\ \log\ 1\cdot 1}$, a fost înlocuit cu zero. Deci, aplicînd formula de transformare a sumelor a lui Abel, obținem

$$\sum_{mn\leqslant x}\frac{\Lambda(m)\ \Lambda(n)}{mn\ \log\ mn}=\sum_{i=2}^{[x]}\frac{1}{\log i}\left(\sum_{n|i}\frac{\Lambda(n)\,\Lambda\left(\frac{i}{n}\right)}{i}\right)=$$

$$=\sum_{k=2}^{[x]}\left(\sum_{l=2}^{k}\sum_{n|l}\frac{\Lambda(n)\,\Lambda\left(\frac{l}{n}\right)}{l}\right)\left(\frac{1}{\log\ k}-\frac{1}{\log\ (k+1)}\right)+$$

$$+\left(\sum_{l=2}^{[x]}\sum_{n|l}\frac{\Lambda(n)\ \ \Lambda\left(\frac{l}{n}\right)}{l}\right)\frac{1}{\log([x]+1)}=$$

$$=\sum_{2\leqslant k\leqslant x}\left(\sum_{2\leqslant l\leqslant k}\sum_{n|l}\frac{\Lambda(n)\ \ \Lambda\left(\frac{l}{n}\right)}{l}\right)\left(\frac{1}{\log\ k}-\frac{1}{\log\ (k+1)}\right)+$$

$$+\left(\sum_{2\leqslant l\leqslant x}\sum_{n|l}\frac{\Lambda(n)\ \ \Lambda\left(\frac{l}{n}\right)}{l}\right)\frac{1}{\log([x]+1)}=$$

$$=\sum_{2\leqslant k\leqslant x}\left(\sum_{mn\leqslant k}\frac{\Lambda(m)\ \ \Lambda(n)}{mn}\right)\left(\frac{1}{\log\ k}-\frac{1}{\log\ (k+1)}\right)+$$

$$+\left(\sum_{mn\leqslant x}\frac{\Lambda(m)\ \Lambda(n)}{mn}\right)\frac{1}{\log([x]+1)}.$$

Ținînd seama de faptul că

$$\frac{1}{\log\ (x+h)}=\frac{1}{\log\ x}-\frac{h}{x\ \log^2 x}+o\left(\frac{1}{x^2}\right),$$

unde h este o constantă, obținem

$$\frac{1}{\log(k+1)}=\frac{1}{\log\ k}-\frac{1}{k\ \log^2 k}+O\left(\frac{1}{k^2}\right).$$

Apoi

$$\left|\frac{1}{\log([x]+1)}-\frac{1}{\log\ x}\right|=\frac{\left|\log\left(\frac{x}{[x]+1}\right)\right|}{\log([x]+1)\log\ x}=\frac{\left|O\left(\frac{x}{[x]+1}\right)\right|}{\log([x]+1)\ \log\ x}=$$

$$=\frac{O(O(1))}{\log([x]+1)\log\ x}=\frac{O(1)}{\log([x]+1)\log\ x}\leqslant\frac{O(1)}{\log^2 x}=O\left(\frac{1}{\log^2 x}\right),$$

deci $\frac{1}{\log\ ([x]+1)}=\frac{1}{\log\ x}+O\left(\frac{1}{\log^2 x}\right)$.

Aşadar

$$\sum_{mn\leqslant x}\frac{\Lambda(m)\ \Lambda(n)}{mn\log mn}=\sum_{2\leqslant k\leqslant x}\left(\frac{1}{2}\log^2 k+O(\log k)\right)\left(\frac{1}{k\log^2 k}+O\left(\frac{1}{k^2}\right)\right)+$$

$$+\left(\frac{1}{2}\log^2 x+O(\log x)\right)\left(\frac{1}{\log x}+O\left(\frac{1}{\log^2 x}\right)\right)=\frac{1}{2}\sum_{2\leqslant k\leqslant x}\frac{1}{k}+$$

$$+\sum_{2\leqslant k\leqslant x}\left(\frac{O(\log k)}{k\log^2 k}+\frac{1}{2}\log^2 k\,O\left(\frac{1}{k^2}\right)+O(\log k)O\left(\frac{1}{k^2}\right)\right)+\frac{1}{2}\log x+$$

$$+\frac{O(\log x)}{\log x}+\left(\frac{1}{2}\log^2 x+O(\log x)\right)O\left(\frac{1}{\log^2 x}\right)=\frac{1}{2}\sum_{2\leqslant k\leqslant x}\frac{1}{k}+$$

$$+\sum_{2\leqslant k\leqslant x}O\left(\frac{1}{k\log k}\right)+\frac{1}{2}\log x+O\left(\frac{\log x}{\log x}\right)+O(\log^2 x)\,O\left(\frac{1}{\log^2 x}\right).$$

Am pus mai sus

$$\frac{O(\log k)}{k\log^2 k}+\frac{1}{2}\log^2 k\,O\left(\frac{1}{k^2}\right)+O(\log k)O\left(\frac{1}{k^2}\right)=$$

$$=O\left(\frac{\log k}{k\log^2 k}\right)+O\left(\frac{\log^2 k}{k^2}\right)+O\left(\log k\,O\left(\frac{1}{k^2}\right)\right)=O\left(\frac{1}{k\log k}\right).$$

Am putut scrie

$$O(\log k)O\left(\frac{1}{k^2}\right)=O\left(\log k O\left(\frac{1}{k^2}\right)\right),$$

deoarece

$$O\left(\frac{1}{k^2}\right)=\frac{1}{\log(k+1)}-\frac{1}{\log k}+\frac{1}{k\log^2 k},$$

iar pentru funcţia

$$k(x)=\frac{1}{\log(x+1)}-\frac{1}{\log x}+\frac{1}{x\log^2 x}$$

există o constantă x_k astfel încît $k(x)\neq 0$ pentru orice x pentru care $x>x_k$. Într-adevăr, am arătat în cadrul demonstraţiei proprietăţii (2) din acest paragraf 14.2, că $\log(x+1)-\log x-\frac{1}{x}<0$

pentru orice x pentru care $x>0$. Deci $\log\left(\frac{x+1}{x}\right)<\frac{1}{x}$.

Dar $\frac{1}{\log(x+1)}<\frac{1}{\log x}$ deci

$$\frac{\log\left(\frac{x+1}{x}\right)}{\log(x+1)\log x}<\frac{1}{x\log^2 x}$$

sau $k(x)>0$ pentru orice x pentru care $x>1$. Deci dacă luăm $x_k=1$, avem $k(x)\neq 0$ pentru orice x pentru care $x>x_k$.

Putem scrie

$O(\log^2 x)O\left(\frac{1}{\log^2 x}\right)=O\left(\log^2 x\,O\left(\frac{1}{\log^2 x}\right)\right)$, deoarece $O\left(\frac{1}{\log^2 x}\right)$ provine din $\frac{1}{\log([x]+1)}=\frac{1}{\log x}+O\left(\frac{1}{\log^2 x}\right)$, iar

$$\frac{1}{\log([x]+1)}-\frac{1}{\log x}=\frac{\log\left(\frac{x}{[x]+1}\right)}{\log([x]+1)\log x}<0$$

pentru orice x pentru care $x>1$ şi deci luînd $x_k=1$ şi $k(x)=\frac{1}{\log([x]+1)}-\frac{1}{\log x}$ avem $k(x)\neq 0$ pentru orice x pentru care $x>x_k$.

Apoi putem scrie că

$$\sum_{2\leqslant k\leqslant x}O\left(\frac{1}{k\log k}\right)=O\left(\sum_{2\leqslant k\leqslant x}\frac{1}{k\log k}\right),$$

deoarece putem scrie

$$\sum_{2\leqslant k\leqslant x}O\left(\frac{1}{k\log k}\right)=\sum_{1\leqslant n\leqslant x-1}O\left(\frac{1}{(n+1)\log(n+1)}\right)$$

şi deci putem aplica relaţia

$$\sum_{1\leqslant n\leqslant x}f(n)h(n)=O\left(\sum_{1\leqslant n\leqslant x}|f(n)||g(n)|\right).$$

unde $f(x)=1$, $g(x)=\dfrac{1}{(x+1)\log(x+1)}$ și $h(x)=O(g(x))$, funcțiile $f(x)$, $g(x)$ fiind definite pentru orice număr natural x și dacă luăm $a=1$ avem $f(a)g(a)\neq 0$. Funcția $h(x)$ este definită pentru orice număr natural x, deoarece

$$h(x-1)=\frac{O(\log x)}{x\log^2 x}+\frac{1}{2}\log^2 x\, O\left(\frac{1}{x^2}\right)+O(\log x)O\left(\frac{1}{x^2}\right),$$

iar pentru $x\geqslant 2$, x fiind număr natural, termenii acestei sume sînt definiți, deoarece $O(\log x)$ și $O\left(\frac{1}{x^2}\right)$ se obțin din

$$\sum_{mn\leqslant x}\frac{\Lambda(m)\ \Lambda(n)}{mn}=\frac{1}{2}\log^2 x+O(\log x),\frac{1}{\log(x+1)}=\frac{1}{\log x}-$$

$$-\frac{1}{x\log^2 x}+O\left(\frac{1}{x^2}\right).$$

Deci

$$\sum_{mn\leqslant x}\frac{\Lambda(m)\ \Lambda(n)}{mn\log mn}=\frac{1}{2}\sum_{2\leqslant k\leqslant x}\frac{1}{k}+O\left(\sum_{2\leqslant k\leqslant x}\frac{1}{k\log k}\right)+\frac{1}{2}\log x+$$

$$+O(1)+O\left(O\left(\frac{\log^2 x}{\log^2 x}\right)\right)=\frac{1}{2}\left(\log x+K_1+O\left(\frac{1}{x}\right)\right)+O\left(\log\log x+\right.$$

$$\left.+K_2+O\left(\frac{1}{x\log x}\right)\right)+\frac{1}{2}\log x+O(1)+O(O(1))=\log x+O(\log\log x).$$

(5) **Relația lui Selberg.** Înainte de a stabili relația lui Selberg, vom demonstra următoarea teoremă:

Teoremă. *Dacă $F(x)$ și $G(x)$ sînt două funcții definite pentru orice x pentru care $x\geqslant 1$ și dacă*

$$G(x)=\sum_{1\leqslant m\leqslant x}F\left(\frac{x}{m}\right)\log x,$$

atunci

$$F(x)\log x+\sum_{1\leqslant n\leqslant x}F\left(\frac{x}{n}\right)\Lambda(n)=\sum_{1\leqslant d\leqslant x}\mu(d)G\left(\frac{x}{d}\right),$$

unde μ este funcția lui Moebius.

Demonstrație. Avem

$$F(x)\log x+\sum_{1\leqslant n\leqslant x}F\left(\frac{x}{n}\right)\Lambda(n)=\sum_{1\leqslant n\leqslant x}F\left(\frac{x}{n}\right)\log\frac{x}{n}\sum_{d\mid n}\mu(d)+$$

$$+\sum_{1\leqslant n\leqslant x}F\left(\frac{x}{n}\right)\sum_{d\mid n}\mu(d)\ \log\frac{n}{d},$$

deoarece în prima sumă dacă $n>1$, avem

$$\sum_{d\mid n}\mu(d)=0,$$

iar dacă $n=1$, avem $\sum_{d\mid n}\mu(d)=1$, iar în a doua sumă

$$\Lambda(n)=\sum_{d\mid n}\mu(d)\ \log\frac{n}{d}.$$

Obținem, mai departe,

$$F(x)\ \log x+\sum_{1\leqslant n\leqslant x}F\left(\frac{x}{n}\right)\Lambda(n)=\sum_{1\leqslant n\leqslant x}F\left(\frac{x}{n}\right)\sum_{d\mid n}\mu(d)\left(\log\frac{x}{n}+\right.$$

$$\left.+\log\frac{n}{d}\right)=\sum_{1\leqslant n\leqslant x}\sum_{d\mid n}F\left(\frac{x}{n}\right)\mu(d)\ \log\frac{x}{d}=$$

$$=\sum_{1\leqslant d\leqslant x}\mu(d)\sum_{1\leqslant t\leqslant\frac{x}{d}}F\left(\frac{x}{dt}\right)\log\frac{x}{d}=\sum_{1\leqslant d\leqslant x}\mu(d)G\left(\frac{x}{d}\right)$$

și deci teorema este demonstrată.

Acum vom demonstra *relația lui Selberg* care este următoarea

$$\Psi(x)\log x+\sum_{1\leqslant n\leqslant x}\Psi\left(\frac{x}{n}\right)\Lambda(n)=2x\log x+O(x).$$

Demonstrație. În relația din teorema precedentă, vom pune în locul lui $F(x)$ pe $F_1(x)=\Psi(x)$ și vom obține

$$\Psi(x)\ \log x+\sum_{1\leqslant n\leqslant x}\Psi\left(\frac{x}{n}\right)\Lambda(n)=\sum_{1\leqslant d\leqslant x}\mu(d)G_1\left(\frac{x}{d}\right),$$

unde

$$G_1(x)=\sum_{1\leqslant m\leqslant x}\Psi\left(\frac{x}{m}\right)\log x=\left(\sum_{1\leqslant m\leqslant x}\sum_{1\leqslant n\leqslant\frac{x}{m}}\Lambda(n)\right)\log x=$$

$$=\left(\sum_{1\leqslant c\leqslant x}\sum_{n|c}\Lambda(n)\right)\log x=\left(\sum_{1\leqslant c\leqslant x}\log c\right)\log x=(x\log x-x+$$

$+O(\log x))\log x=x\log^2 x-x\log x+O(\log^2 x)=x\log^2 x-x\log x+$ $+O(\sqrt{x})$, deoarece avem $\log^2 x=O(\sqrt{x})$.

În relația din teorema precedentă, vom pune în locul lui $F(x)$ pe $F_2(x)=x-K$, unde K este o constantă și vom obține

$$(x-K)\log x+\sum_{1\leqslant n\leqslant x}\left(\frac{x}{n}-K\right)\Lambda(n)=\sum_{1\leqslant d\leqslant x}\mu(d)\,G_2\left(\frac{x}{d}\right),$$

unde

$$G_2(x)=\sum_{1\leqslant m\leqslant x}\left(\frac{x}{m}-K\right)\log x=\left(\sum_{1\leqslant m\leqslant x}\frac{1}{m}\right)x\log x-K[x]\log x=$$

$$=\left(\log x+C+O\left(\frac{1}{x}\right)\right)x\log x-K[x]\log x=x\log^2 x+(Cx-$$

$$-K[x])\log x+O(\log x).$$

Dacă luăm $K=C+1$, obținem

$(Cx-K[x])\log x=(Cx-C[x]-[x])\log x=C(x-[x])\log x=x\log x+$ $+(x-[x])\log x=C\{x\}\log x-x\log x+\{x\}\log x=-x\log x+$ $+O(\log x)$, deoarece $C\{x\}\log x+\{x\}\log x=O(\log x)$, având $|C\{x\}\log x+\{x\}\log x|<(C+1)\log x=O(\log x)$. Însă avem $\log x=$ $=O(\sqrt{x})$, deci

$$G_2(x)=x\log^2 x-x\log x+O(\sqrt{x}).$$

Se deduce că

$$G_1(x)-G_2(x)=O(\sqrt{x}).$$

Deci

$$\Psi(x)\log x+\sum_{1\leqslant n\leqslant x}\Psi\left(\frac{x}{n}\right)\Lambda(n)-(x-C-1)\log x-\sum_{1\leqslant n\leqslant x}\left(\frac{x}{n}-\right.$$

$$\left.-C-1\right)\Lambda(n)=\sum_{1\leqslant d\leqslant x}\mu(d)O\left(\sqrt{\frac{x}{d}}\right).$$

Avem

$$\left|\sum_{1\leqslant d\leqslant x}\mu(d)O\left(\sqrt{\frac{x}{d}}\right)\right|\leqslant\sum_{1\leqslant d\leqslant x}O\left(\sqrt{\frac{x}{d}}\right)=O\left(\sum_{1\leqslant d\leqslant x}\sqrt{\frac{x}{d}}\right)=$$

$$=O\left(\sqrt{x}\left(2\sqrt{x}+C+O\left(\frac{1}{\sqrt{x}}\right)\right)\right)=O(2x+C\sqrt{x}+O(1))=O(x),$$

deci

$$\sum_{1\leqslant d\leqslant x}\mu(d)O\left(\sqrt{\frac{x}{d}}\right)=O(x).$$

Am putut scrie

$$\sum_{1\leqslant d\leqslant x}O\left(\sqrt{\frac{x}{d}}\right)=O\left(\sum_{1\leqslant d\leqslant x}\sqrt{\frac{x}{d}}\right),$$

deoarece putem aplica relația

$$\sum_{1\leqslant n\leqslant x}f(n)h\left(\frac{x}{n}\right)=O\left(\sum_{1\leqslant n\leqslant x}\left|f(n)\right|\left|g\left(\frac{x}{n}\right)\right|\right),$$

funcția $f(x)=1$ fiind definită pentru orice număr natural x, funcția $g(x)=\sqrt{x}$ fiind definită și $|g(x)|\geqslant 1$ pentru orice x pentru care $x\geqslant 1$, funcția $f(x)$ fiind diferită de zero măcar pentru un număr natural x. Funcția $h(x)=O(\sqrt{x})$ este definită și mărginită pe intervalul $[1,\alpha]$ pentru orice α pentru care $\alpha\geqslant 1$, deoarece

$$h(x)=G_1(x)-G_2(x).$$

În felul acesta am obținut că

$$\Psi(x)\log x+\sum_{1\leqslant n\leqslant x}\Psi\left(\frac{x}{n}\right)\Lambda(n)=(x-C-1)\log x+\sum_{1\leqslant n\leqslant x}\left(\frac{x}{n}-C-\right.$$

$$-1)\Lambda(n)+O(x)=x\log x-(C+1)\log x+x\sum_{1\leqslant n\leqslant x}\frac{\Lambda(n)}{n}-$$

$$-(C+1)\sum_{1\leqslant n\leqslant x}\Lambda(n)+O(x)=x\log x+O(x)+x(\log x+O(1))-(C+$$

$$+1)\,\Psi(x)+O(x)=2x\log x+O(x).$$

Cu aceasta, relația lui Selberg a fost demonstrată.

Observație. Relația lui Selberg poate fi scrisă sub forma

$$\sum_{mn\leqslant x}\Lambda(m)\,\Lambda(n)=2x\log x-\Psi(x)\log x+O(x)$$

unde suma $\sum_{mn\leqslant x}\Lambda(m)\,\Lambda(n)$ se face după toate perechile (m, n) de numere naturale al căror produs mn este cel mult egal cu x, fiecare pereche (m, n) fiind luată o singură dată. Transformarea indicată a relației lui Selberg poate fi efectuată, deoarece

$$\sum_{mn\leqslant x}\Lambda(m)\,\Lambda(n)=\sum_{1\leqslant n\leqslant x}\ \sum_{1\leqslant m\leqslant\frac{x}{n}}\Lambda(m)\,\Lambda(n)=$$

$$=\sum_{1\leqslant n\leqslant x}\Big(\sum_{1\leqslant m\leqslant\frac{x}{n}}\Lambda(m)\Big)\Lambda(n)=\sum_{1\leqslant n\leqslant x}\Psi\Big(\frac{x}{n}\Big)\Lambda(n).$$

Pentru acest motiv am inclus relația lui Selberg printre evaluări asimptotice ale unor sume în care intervine funcția lui Mangoldt.

(6) $$\sum_{mn\leqslant x}\frac{\Lambda(m)\ \Lambda(n)}{\log mn}=2x-\Psi(x)+o(x),$$

unde suma $\sum_{mn\leqslant x}\frac{\Lambda(m)\ \Lambda(n)}{\log mn}$ *se face pentru toate perechile de numere naturale* (m, n) *pentru care produsul* mn *este cel mult egal cu un număr real* x, *fiecare pereche* (m, n) *fiind luată o singură dată. Termenul* $\frac{\Lambda(1)\ \Lambda(1)}{\log 1\cdot 1}$ *care nu are sens, avînd forma* $\frac{0}{0}$, *este presupus înlocuit cu* 0.

Demonstrație. Deoarece în suma considerată termenul $\frac{\Lambda(1)\ \Lambda(1)}{\log 1\cdot 1}$ este înlocuit cu zero, putem scrie

$$\sum_{mn\leqslant x}\frac{\Lambda(m)\ \Lambda(n)}{\log mn}=\sum_{1<m\leqslant x}\ \sum_{1\leqslant n\leqslant\frac{x}{m}}\frac{\Lambda(m)\ \Lambda(n)}{\log mn}=$$

$$=\sum_{1\leqslant c\leqslant x}\ \sum_{n|c}\frac{\Lambda\left(\frac{c}{n}\right)\Lambda(n)}{\log c}=\sum_{2\leqslant c\leqslant x}\ \sum_{n|c}\frac{\Lambda\left(\frac{c}{n}\right)\Lambda(n)}{\log c}=$$

$$=\sum_{i=2}^{[x]}\ \sum_{n|i}\frac{\Lambda\left(\frac{i}{n}\right)\Lambda(n)}{\log i}.$$

Aplicînd formula de transformare a sumelor a lui Abel, obținem cu $a_i=\sum_{n|i}\Lambda\left(\frac{i}{n}\right)\Lambda(n)$ și $b_i=\frac{1}{\log i}$, că

$$\sum_{mn\leqslant x}\frac{\Lambda(m)\ \Lambda(n)}{\log mn}=\sum_{k=2}^{[x]}\Big(\sum_{l=2}^{k}\ \sum_{n|l}\Lambda\Big(\frac{l}{n}\Big)\ \Lambda(n)\Big)\Big(\frac{1}{\log k}-\frac{1}{\log(k+1)}\Big)+$$

$$+\Big(\sum_{l=2}^{[x]}\ \sum_{n|l}\Lambda\Big(\frac{l}{n}\Big)\Lambda(n)\Big)\frac{1}{\log([x]+1)}=\sum_{2\leqslant k\leqslant x}\Big(\sum_{mn\leqslant k}\Lambda(m)\Lambda(n)\Big)\cdot$$

$$\cdot\Big(\frac{1}{\log k}-\frac{1}{\log(k+1)}\Big)+\Big(\sum_{mn\leqslant x}\Lambda(m)\ \Lambda(n)\Big)\frac{1}{\log([x]+1)}.$$

Ca și în cazul demonstrației proprietății (4) din acest paragraf 14.2, obținem

$$\frac{1}{\log(k+1)}=\frac{1}{\log k}-\frac{1}{k\log^2 k}+O\Big(\frac{1}{k^2}\Big),\quad\frac{1}{\log([x]+1)}=$$

$$=\frac{1}{\log x}+O\Big(\frac{1}{\log^2 x}\Big).$$

Deci

$$\sum_{mn\leqslant x}\frac{\Lambda(m)\ \Lambda(n)}{\log mn}=\sum_{2\leqslant k\leqslant x}\Big(2k\log k-\Psi(k)\log k+O(k)\Big)\Big(\frac{1}{k\log^2 k}+$$

$$+O\left(\frac{1}{k^2}\right)\Big)+(2x\log x-\Psi(x)\log x+O(x))\left(\frac{1}{\log x}+O\left(\frac{1}{\log^2 x}\right)\right)=$$

$$=2\sum_{2\leqslant k\leqslant x}\frac{1}{\log k}+\sum_{2\leqslant k\leqslant x}\Big(-\frac{\Psi(k)}{k\log k}+\frac{O(k)}{k\log^2 k}+2k\log k\,O\left(\frac{1}{k^2}\right)-$$

$$-\Psi(k)\log k\,O\left(\frac{1}{k^2}\right)+O(k)O\left(\frac{1}{k^2}\right)\Big)+2x-\Psi(x)+\frac{O(x)}{\log x}+(2x\log x-$$

$$-\Psi(x)\log x+O(x))\,O\left(\frac{1}{\log^2 x}\right)=2\sum_{2\leqslant k\leqslant x}\frac{1}{\log k}+\sum_{2\leqslant k\leqslant x}O\left(\frac{1}{\log k}\right)+$$

$$+2x-\Psi(x)+O\left(\frac{x}{\log x}\right)+O(x\log x)O\left(\frac{1}{\log^2 x}\right).$$

Am pus mai sus

$$-\frac{\Psi(k)}{k\log k}+\frac{O(k)}{k\log^2 k}+2k\log k\,O\left(\frac{1}{k^2}\right)-\Psi(k)\log k\,O\left(\frac{1}{k^2}\right)+$$

$$+O(k)O\left(\frac{1}{k^2}\right)=O\left(\frac{k}{k\log k}\right)+O\left(\frac{k}{k\log^2 k}\right)+O\left(\frac{k\log k}{k^2}\right)+$$

$$+O\left(k\log k\,O\left(\frac{1}{k^2}\right)\right)+O\left(kO\left(\frac{1}{k^2}\right)\right)=O\left(\frac{1}{\log k}\right).$$

Am putut scrie

$$\Psi(k)\log k\,O\left(\frac{1}{k^2}\right)=O\left(k\log k\,O\left(\frac{1}{k^2}\right)\right)\text{ și }O(k)O\left(\frac{1}{k^2}\right)=O\left(kO\left(\frac{1}{k^2}\right)\right),$$

deoarece

$$O\left(\frac{1}{k^2}\right)=\frac{1}{\log(k+1)}-\frac{1}{\log k}+\frac{1}{k\log^2 k},$$

iar pentru funcția

$$k(x)=\frac{1}{\log(x+1)}-\frac{1}{\log x}+\frac{1}{x\log^2 x}$$

există o constantă x_k astfel încît $k(x)\neq 0$ pentru orice x pentru care $x\geqslant x_k$, după cum am demonstrat acest lucru în cadrul demonstrației proprietății (4) din acest paragraf 14.2.

Putem scrie

$$O(x\log x)O\left(\frac{1}{\log^2 x}\right)=O\left(x\log xO\left(\frac{1}{\log^2 x}\right)\right),$$

deoarece $O\left(\frac{1}{\log^2 x}\right)$ provine din

$$\frac{1}{\log([x]+1)}=\frac{1}{\log x}+O\left(\frac{1}{\log^2 x}\right),$$

iar pentru funcția $k(x)=\frac{1}{\log([x]+1)}-\frac{1}{\log x}$ există o constantă x_k astfel încît $k(x)\neq 0$ pentru orice x pentru care $x>x_k$, după cum am demonstrat acest lucru în cadrul demonstrației proprietății (4) din acest paragraf 14.2.

Apoi putem scrie

$$\sum_{2\leqslant k\leqslant x}O\left(\frac{1}{\log k}\right)=O\left(\sum_{2\leqslant k\leqslant x}\frac{1}{\log k}\right),$$

deoarece putem scrie $\sum_{2\leqslant k\leqslant x}O\left(\frac{1}{\log k}\right)=\sum_{1\leqslant n\leqslant x-1}O\left(\frac{1}{\log(n+1)}\right)$ și deci putem aplica relația

$$\sum_{1\leqslant n\leqslant x}f(n)h(n)=O\Big(\sum_{1\leqslant n\leqslant x}|f(n)||g(n)|\Big),$$

unde $f(x)=1$, $g(x)=\frac{1}{\log(x+1)}$ și $h(x)=O(g(x))$, funcțiile $f(x)$, $g(x)$ și $h(x)$ fiind definite pentru orice număr natural x și dacă luăm $a=1$, avem $f(a)g(a)\neq 0$. Funcția $h(x)$ este definită pentru orice număr natural x, deoarece

$$h(x-1)=-\frac{\Psi(x)}{x\log x}+\frac{O(x)}{x\log^2 x}+2x\log x\,O\left(\frac{1}{x^2}\right)-$$

$$-\Psi(x)\log x\,O\left(\frac{1}{x^2}\right)+O(x)O\left(\frac{1}{x^2}\right),$$

iar pentru x natural, $x\geqslant 2$, termenii acestei sume sînt definiți, avînd

$$\sum_{mn\leqslant x}\Lambda(m)\Lambda(n)=2x\log x-\Psi(x)\log x+O(x),\ \frac{1}{\log(x+1)}=\frac{1}{\log x}-$$

$$-\frac{1}{x\log^2 x}+O\left(\frac{1}{x^2}\right).$$

Deci

$$\sum_{mn\leqslant x}\frac{\Lambda(m)\ \Lambda(n)}{\log\ mn}=2\sum_{2\leqslant k\leqslant x}\frac{1}{\log\ k}+O\left(\sum_{2\leqslant k\leqslant x}\frac{1}{\log\ k}\right)+2x-\Psi(x)+$$

$$+O\left(\frac{x}{\log\ x}\right)=2o(x)+O(o(x))+2x-\Psi(x)+O(o(x))=2x-\Psi(x)+o(x).$$

$$(7)\sum_{mn\leqslant x}\Lambda(m)\,\Lambda(n)+\sum_{mn\leqslant x}\frac{\Lambda(m)\ \Lambda(n)}{\log\ mn}\Psi\left(\frac{x}{mn}\right)=2x\log\ x+$$

$$+o(x\ \log\ x).$$

Demonstrație.

$$\sum_{mn\leqslant x}\Lambda(m)\ \Lambda(n)=\sum_{1\leqslant n\leqslant x}\Psi\left(\frac{x}{n}\right)\Lambda(n),$$

după cum rezultă din observația la relația lui Selberg. Dacă scoatem pe $\Psi\left(\frac{x}{n}\right)$ din proprietatea (6), obținem

$$\sum_{mn\leqslant x}\Lambda(m)\,\Lambda(n)=\sum_{1\leqslant n\leqslant x}\left(2\frac{x}{n}-\sum_{mr\leqslant\frac{x}{n}}\frac{\Lambda(m)\ \Lambda(r)}{\log\ mr}+o\left(\frac{x}{n}\right)\right)\Lambda(n)=$$

$$=2x\sum_{1\leqslant n\leqslant x}\frac{\Lambda(n)}{n}-\sum_{1\leqslant n\leqslant x}\left(\sum_{mr\leqslant\frac{x}{n}}\frac{\Lambda(m)\ \Lambda(r)}{\log\ mr}\right)\Lambda(n)+$$

$$+\sum_{1\leqslant n\leqslant x}o\left(\frac{x}{n}\right)\Lambda(n).$$

Însă

$$\sum_{1\leqslant n\leqslant x}\left(\sum_{mr\leqslant\frac{x}{n}}\frac{\Lambda(m)\ \Lambda(r)}{\log\ mr}\right)\Lambda(n)=\sum_{1\leqslant n\leqslant x}\sum_{1\leqslant m\leqslant\frac{x}{n}}\sum_{1\leqslant r\leqslant\frac{x}{mn}}\frac{\Lambda(m)\ \Lambda(r)}{\log\ mr}\Lambda(n)=$$

$$=\sum_{1\leqslant m\leqslant x}\sum_{1\leqslant n\leqslant\frac{x}{m}}\sum_{1\leqslant r\leqslant\frac{x}{mn}}\frac{\Lambda(m)\ \Lambda(r)}{\log\ mr}\Lambda(n)=$$

$$=\sum_{1\leqslant m\leqslant x}\sum_{1\leqslant r\leqslant\frac{x}{m}}\sum_{1\leqslant n\leqslant\frac{x}{mr}}\frac{\Lambda(m)\ \Lambda(r)}{\log\ mr}\Lambda(n)=$$

$$=\sum_{1\leqslant m\leqslant x}\sum_{1\leqslant r\leqslant\frac{x}{m}}\frac{\Lambda(m)\ \Lambda(r)}{\log\ mr}\left(\sum_{1\leqslant n\leqslant\frac{x}{mr}}\Lambda(n)\right)=$$

$$=\sum_{mr\leqslant x}\frac{\Lambda(m)\ \Lambda(r)}{\log\ mr}\Psi\left(\frac{x}{mr}\right).$$

Deci

$$\sum_{mn\leqslant x}\Lambda(m)\ \Lambda(n)+\sum_{mn\leqslant x}\frac{\Lambda(m)\ \Lambda(n)}{\log\ mn}\Psi\left(\frac{x}{mn}\right)=2x\sum_{1\leqslant n\leqslant x}\frac{\Lambda(n)}{n}+$$

$$+\sum_{1\leqslant n\leqslant x}o\left(\frac{x}{n}\right)\Lambda(n).$$

Punînd $h(x)=o(x)$, există o constantă C_1 astfel încît $x>0$ pentru orice x pentru care $x\geqslant C_1$, iar $\lim\limits_{x\to\infty}\frac{h(x)}{x}=0$. Se vede că putem lua $C_1=0$. Deci fiind dat un număr real ε pozitiv, există o constantă C_2 astfel încît $\left|\frac{h(x)}{x}-0\right|<\varepsilon$, de unde rezultă că $|h(x)|<\varepsilon x$ pentru orice x pentru care $x\geqslant C_2$. Putem alege pe C_2 astfel încît $C_2>1$. Din această cauză vom scrie

$$\sum_{1\leqslant n\leqslant x}o\left(\frac{x}{n}\right)\Lambda(n)=\sum_{1\leqslant n<\frac{x}{C_2}}o\left(\frac{x}{n}\right)\Lambda(n)+\sum_{\frac{x}{C_2}\leqslant n\leqslant x}o\left(\frac{x}{n}\right)\Lambda(n).$$

Atunci cînd $1\leqslant n<\frac{x}{C_2}$, avem $C_2<\frac{x}{n}$, deci

$$\left|\sum_{1\leqslant n<\frac{x}{C_2}}o\left(\frac{x}{n}\right)\Lambda(n)\right|\leqslant\sum_{1\leqslant n<\frac{x}{C_2}}\left|o\left(\frac{x}{n}\right)\right|\Lambda(n)<\varepsilon x\sum_{1\leqslant n<\frac{x}{C_2}}\frac{\Lambda(n)}{n}\leqslant$$

$$\leqslant\varepsilon x\sum_{1\leqslant n\leqslant x}\frac{\Lambda(n)}{n}.$$

ultima majorare făcîndu-se datorită faptului că din $1<C_2$ deducem $\frac{1}{C_2}<1$, deci $\frac{x}{C_2}<x$, iar $\frac{\Lambda(n)}{n}\geqslant 0$.

Deci fiind dat ε real pozitiv, avem $\left|\sum_{1\leqslant n<\frac{x}{C_2}} o\left(\frac{x}{n}\right)\Lambda(n)\right| <$

$<\varepsilon x\sum_{1\leqslant n\leqslant x}\frac{\Lambda(n)}{n}$, adică

$$\left|\frac{\sum_{1\leqslant n<\frac{x}{C_2}} o\left(\frac{x}{n}\right)\Lambda(x)}{x\sum_{1\leqslant n<x}\frac{\Lambda(n)}{n}}-0\right|<\varepsilon$$

pentru orice x pentru care $x>2$, această condiție impunîndu-se ca $x\sum_{1\leqslant n\leqslant x}\frac{\Lambda(n)}{n}\neq 0$, deci

$$\sum_{1\leqslant n<\frac{x}{C_2}} o\left(\frac{x}{n}\right)\Lambda(n)=o\left(x\sum_{1\leqslant n\leqslant x}\frac{\Lambda(n)}{n}\right).$$

Atunci cînd $\frac{x}{C_2}\leqslant n\leqslant x$, avem $1\leqslant\frac{x}{n}\leqslant C_2$, deci

$$\left|o\left(\frac{x}{n}\right)\right|\leqslant\sum_{mr\leqslant\frac{x}{n}}\frac{\Lambda(m)\ \Lambda(r)}{\log\ mr}+2\frac{x}{n}+\Psi\left(\frac{x}{n}\right)\leqslant\sum_{mr\leqslant C_2}\frac{\Lambda(m)\ \Lambda(r)}{\log\ mr}+2C_2+$$

$+\Psi(C_2)=C$, deci $\left|o\left(\frac{x}{n}\right)\right|\leqslant C$.

Așadar,

$$\left|\sum_{\frac{x}{C_2}\leqslant n\leqslant x} o\left(\frac{x}{n}\right)\Lambda(n\right|\leqslant C\sum_{\frac{x}{C_2}\leqslant n\leqslant x}\Lambda(n)\leqslant C\sum_{1\leqslant n\leqslant x}\Lambda(n)=C\Psi(x)=O(x).$$

Deci

$$\sum_{\frac{x}{C_2}\leqslant n\leqslant x} o\left(\frac{x}{n}\right)\Lambda(n)=O(x).$$

Rezultă că

$$\sum_{1\leqslant n\leqslant x} o\left(\frac{x}{n}\right)\Lambda(n)=o\left(x\sum_{1\leqslant n\leqslant x}\frac{\Lambda(n)}{n}\right)+O(x)=o(x(\log\ x+O(1)))+O(x)=$$

$$=o(O(x\ \log\ x))+O(o(x\ \log\ x))=o(x\ \log\ x).$$

Am obținut

$$\sum_{mn\leqslant x}\Lambda(m)\ \Lambda(n)+\sum_{mn\leqslant x}\frac{\Lambda(m)\ \Lambda(n)}{\log\ mn}\Psi\left(\frac{x}{mn}\right)=2x(\log\ x+O(1))+$$

$$+o(x\ \log\ x)=2x\ \log\ x+o(x\ \log\ x)$$

și cu aceasta relația considerată a fost demonstrată.

(8) $$\Psi(x)\log\ x=\sum_{mn\leqslant x}\frac{\Lambda(m)\ \Lambda(n)}{\log\ mn}\Psi\left(\frac{x}{mn}\right)+o(x\ \log\ x).$$

Demonstrație. Luînd relația lui Selberg sub forma

$$\sum_{mn\leqslant x}\Lambda(m)\ \Lambda(n)=2x\ \log\ x-\Psi(x)\ \log\ x+O(x),$$

relația (7) devine

$$2x\ \log\ x-\Psi(x)\log\ x+O(x)+\sum_{mn\leqslant x}\frac{\Lambda(m)\ \Lambda(n)}{\log\ mn}\Psi\left(\frac{x}{mn}\right)=2x\log x+$$

$$+o(x\ \log\ x),$$

de unde rezultă relația (8).

14.3. Evaluări asimptotice ale funcției $\pi(x)$

(1) $$\pi(x)=O\left(\frac{x}{\log\log x}\right).$$

Demonstrație. Dacă p_r este al r-lea număr prim pozitiv și $p_r<x$, atunci $\pi(x)=r+N$, unde N este numărul numerelor prime pozitive mai mari ca p_r și cel mult egale cu x. Avem $N\leqslant\varphi(x, r)$, deoa-

rece numerele naturale numărate în $\varphi(x, r)$ sînt nedivizibile cu $p_1, \ldots, p_r$ ca și numerele prime pozitive mai mari ca p_r și cel mult egale cu x și sînt și ele cel mult egale cu x. Dacă $p_r \geqslant x$, atunci $\pi(x) \leqslant r$, deci, în toate cazurile

$$\pi(x) \leqslant r + \varphi(x, r).$$

Avem

$$\varphi(x, r) = \sum_{d \mid p_1 \ldots p_r} \mu(d) \left[\frac{x}{d}\right] = \sum_{d \mid p_1 \ldots p_r} \mu(d) \left(\frac{x}{d} - \left\{\frac{x}{d}\right\}\right) =$$

$$= \sum_{d \mid p_1 \ldots p_r} \mu(d) \frac{x}{d} - \sum_{d \mid p_1 \ldots p_r} \mu(d) \left\{\frac{x}{d}\right\} \leqslant x \sum_{d \mid p_1 \ldots p_r} \frac{\mu(d)}{d} +$$

$$+ \sum_{d \mid p_1 \ldots p_r} \left\{\frac{x}{d}\right\} < x \prod_{p \leqslant p_r} \left(1 - \frac{1}{p}\right) + 2^r,$$

unde produsul este extins la toate numerele prime pozitive cel mult egale cu p_r. Deci

$$\varphi(x, r) < x \prod_{p \leqslant p_r} \left(1 - \frac{1}{p}\right) + 2^r.$$

Pentru a ajunge la această evaluare, am ținut seama de faptul că

$$\prod_{p \leqslant p_r} \left(1 - \frac{1}{p}\right) = \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) = \sum_{d \mid p_1 \ldots p_r} \frac{\mu(d)}{d}, \quad \left\{\frac{x}{d}\right\} < 1,$$

$$\sum_{d \mid p_1 \ldots p_r} \left\{\frac{x}{d}\right\} \leqslant 2^r, \quad -\mu(d) \leqslant 1,$$

Prima dintre aceste relații am demonstrat-o pe la sfîrșitul paragrafului 8.2, iar celelalte rezultă din definiția părții fracționare, a funcției lui Moebius și a numărului divizorilor pozitivi ai unui număr întreg.

Mai departe avem

$$\left(\prod_{p \leqslant p_r} \left(1 - \frac{1}{p}\right)\right)^{-1} = \prod_{i=1}^{r} \frac{1}{1 - \frac{1}{p_i}} = \prod_{i=1}^{r} \left(1 + \frac{1}{p_i} + \frac{1}{p_i^2} + \ldots\right) =$$

$$= \sum \frac{1}{p_{i_1}^{\alpha_1} \ldots p_{i_s}^{\alpha_s}} > \sum_{1 \leqslant n \leqslant p_r} \frac{1}{n},$$

deoarece orice număr natural cel mult egal cu p_r se scrie sub forma $p_{i_1}^{\alpha_1} \ldots p_{i_s}^{\alpha_s}$, unde $p_{i_1}, \ldots, p_{i_s}$ sînt numere prime pozitive cel mult egale cu p_r, iar $\alpha_1, \ldots, \alpha_s$ sînt numere întregi nenegative. Prin

$$\sum \frac{1}{p_{i_1}^{\alpha_1} \ldots p_{i_s}^{\alpha_s}}$$

am înțeles suma tuturor inverselor numerelor naturale de forma $p_{i_1}^{\alpha_1} \ldots p_{i_s}^{\alpha_s}$, unde $p_{i_1} \ldots, p_{i_s}$ sînt numere prime pozitive cel mult egale cu p_r, iar $\alpha_1, \ldots, \alpha_s$ sînt numere întregi nenegative. Dar

$$\sum_{1 \leqslant n \leqslant p_r} \frac{1}{n} = \log p_r + C + O\left(\frac{1}{p_r}\right),$$

C fiind o constantă pozitivă. Din definiția lui $O\left(\frac{1}{p_r}\right)$ rezultă că există două constante pozitive C_1 și C_2 astfel încît $\left| O\left(\frac{1}{p_r}\right)\right| < C_1 \frac{1}{p_r}$ îndată ce $p_r > C_2$. Deci dacă $p_r > C_2$, atunci

$$-C_1 \frac{1}{p_r} < O\left(\frac{1}{p_r}\right) < C_1 \frac{1}{p_r}$$

și deci pentru $p_r > C_2$ avem

$$C - C_1 \frac{1}{p_r} < C + O\left(\frac{1}{p_r}\right).$$

Putem face ca $C - C_1 \frac{1}{p_r} > 0$ luînd $p_r > \frac{C_1}{C}$. Deci dacă $p_r > \max\left(C_2, \frac{C_1}{C}\right)$ atunci $C + O\left(\frac{1}{p_r}\right) > 0$ și

$$\sum_{1 \leqslant n \leqslant p_r} \frac{1}{n} > \log p_r.$$

Fie N un număr natural astfel încît $p_N \geqslant \max\left(C_2, \frac{C_1}{C}\right)$. Atunci pentru orice număr natural r pentru care $r > N$ avem

$$\prod_{p \leqslant p_r} \left(1 - \frac{1}{p}\right) < \frac{1}{\log p_r} < \frac{1}{\log r},$$

ultima inegalitate fiind adevărată, deoarece $p_r > r$. Deci pentru orice număr natural r pentru care $r > N$, avem

$$\varphi(x, r) < \frac{x}{\log r} + 2^r.$$

Dar $\pi(x) \leqslant r + \varphi(x, r) < 2^r + \varphi(x, r)$, deoarece $r < 2^r$, avînd $2^r = (1+1)^r = 1 + C_r^1 + \ldots = 1 + r + \ldots > r$. Deci pentru orice r pentru care $r > N$, avem

$$\pi(x) < \frac{x}{\log r} + 2^{r+1}.$$

Deci avem și

$$\pi(x) < \frac{x}{\log(r+1)} + 2^{r+2}.$$

Dacă y este un număr real astfel încît $r \leqslant y \leqslant r+1$, atunci $2^r \leqslant 2^y$ și $\log y \leqslant \log(r+1)$, deci

$$\pi(x) < \frac{x}{\log(r+1)} + 2^{r+2} \leqslant \frac{x}{\log y} + 2^{y+2},$$

pentru orice y real astfel încît $y > N$. Fiind dat acum x putem determina pe y cu ajutorul relației $x = e^c$ unde c este o constantă pozitivă. Deci pentru x pentru care $x > e^{\frac{N}{c}}$ avem

$$\pi(x) < \frac{x}{\log(c \log x)} + 4 \cdot 2^{c \log x}.$$

Însă $2^{c \log x} = x^{c \log 2}$, deoarece prin logaritmare se obține identitatea $(c \log x) \log 2 = (c \log 2) \log x$. Deci

$$\lim_{x\to\infty} \frac{\frac{x}{\log(c \log x)} + 4 \cdot 2^{c \log x}}{\frac{x}{\log \log x}} = \lim_{x\to\infty} \frac{x}{\log c + \log \log x} \frac{\log \log x}{x} +$$

$$+ \lim_{x\to\infty} 4x^{c \log 2} \frac{\log \log x}{x} = \lim_{x\to\infty} \frac{1}{\frac{\log c}{\log \log x} + 1} + \lim_{x\to\infty} 4 \frac{\log \log x}{x^{1-c \log 2}} =$$

$$= 1 + \lim_{x\to\infty} 4 \frac{\frac{1}{x \log x}}{(1 - c \log 2) x^{-c \log 2}} =$$

$$= 1 + \lim_{x\to\infty} 4 \frac{1}{(1 - c \log 2) x^{1-c \log 2} \log x} = 1,$$

deoarece constanta pozitivă c o putem alege astfel încît $0 < c < \frac{1}{\log 2}$, deci astfel încît $1 - c \log 2 > 0$. Asta înseamnă că

$$\frac{x}{\log(c \log x)} + 4 \cdot 2^{c \log x} = O\left(\frac{x}{\log \log x}\right),$$

deoarece pentru orice x pentru care $x > e$ avem $\frac{x}{\log \log x} > 0$.

Deci $\pi(x) = O\left(\frac{x}{\log \log x}\right)$, deoarece $0 < \pi(x) < O\left(\frac{x}{\log \log x}\right)$.

(2) $\pi(x) = o(x)$.

Demonstrație. Avem $\frac{x}{\log \log x} = o(x)$, deci $\pi(x) = O(o(x)) = o(x)$.

Observație. Această proprietate poate fi interpretată în sensul că aproape toate numerele naturale sînt compuse, deoarece raportul dintre numărul $\pi(n)$ al numerelor prime aflate printre primele n numere naturale și numărul n al primelor n numere naturale tinde către zero cînd n tinde la infinit.

14.4. Funcția $\vartheta(x)$

Definiție. *Funcția $\vartheta(x)$ este definită prin*

$$\vartheta(x) = \sum_{p \leqslant x} \log p$$

suma fiind extinsă la toate numerele prime pozitive, diferite două cîte două, cel mult egale cu un număr real x.

Proprietăţi ale funcţiei $\vartheta(x)$.

(1) $\Psi(x)=\sum_{r=1}^{\left[\frac{\log x}{\log 2}\right]}\vartheta(x^{\frac{1}{r}})$.

Demonstraţie.

$$\Psi(x)=\sum_{1\leqslant n\leqslant x}\Lambda(n)=\sum_{p\leqslant x}\log p+\sum_{p^2\leqslant x}\log p+\ldots=\sum_{!p\leqslant x}\log p+$$

$$+\sum_{p\leqslant\sqrt{x}}\log p+\ldots=\vartheta(x)+\vartheta(x^{\frac{1}{2}})+\ldots=\sum_{r=1}^{\left[\frac{\log x}{\log 2}\right]}\vartheta(x^{\frac{1}{r}}),$$

deoarece ultima sumă de tipul $\sum_{p^r\leqslant x}\log p$ este $\sum_{p^k\leqslant x}\log p$, unde numai $p=2$ satisface inegalitatea $p^k\leqslant x$, iar $x<2^{k+1}$, deci $2^k\leqslant x<2^{k+1}$, adică $k=\left[\frac{\log x}{\log 2}\right]$, prin $\sum_{p^r\leqslant x}\log p$ înţelegînd o sumă de termeni de forma $\log p$ extinsă la toate numerele prime pozitive p, diferite două cîte două, astfel încît $p^r\leqslant x$, r fiind un număr natural, acelaşi pentru toate numerele prime considerate. Avem $\sum_{p^r\leqslant x}\log p=$ $=\sum_{p\leqslant x^{1/r}}\log p$, deoarece relaţiile $p^r\leqslant x$ şi $p\leqslant x^{1/r}$ sînt echivalente în condiţiile arătate mai sus.

(2) $\Psi(x)=\vartheta(x)+O(x^{1/2}\log^2 x)$.

Demonstraţie. Pentru $r\geqslant 2$ avem

$$\vartheta(x^{1/r})=\sum_{p\leqslant x^{1/r}}\log p\leqslant\sum_{p\leqslant x^{1/r}}\log x^{1/r}=\frac{1}{r}\sum_{p\leqslant x^{1/r}}\log x<$$

$$<\sum_{p\leqslant x^{1/r}}\log x<[x^{1/r}]\log x\leqslant x^{1/r}\log x\leqslant x^{1/2}\log x.$$

Deci

$$\Psi(x)=\vartheta(x)+\sum_{r=2}^{\left[\frac{\log x}{\log 2}\right]}\vartheta(x^{1/r}),$$

unde

$$\left|\sum_{r=2}^{\left[\frac{\log x}{\log 2}\right]}\vartheta(x^{1/r})\right|<\sum_{r=2}^{\left[\frac{\log x}{\log 2}\right]}x^{1/2}\log x<\left[\frac{\log x}{\log 2}\right]x^{1/2}\log x\leqslant$$

$$\leqslant\frac{x^{1/2}\log^2 x}{\log 2}=O(x^{1/2}\log^2 x),$$

deci proprietatea considerată este demonstrată.

(3) $\Psi(x)=\vartheta(x)+o(x)$.

Demonstraţie. Avem $\log^2 x=o(x^{1/2})$ şi ţinînd seama de proprietatea (2) obţinem proprietatea (3), deoarece $O(x^{1/2}\log^2 x)=$ $=O(x^{1/2}o(x^{1/2}))=O(o(x))=o(x)$.

(4) $\vartheta(x)=O(x)$.

Demonstraţie. Din $\Psi(x)=\vartheta(x)+o(x)$ şi $\Psi(x)=O(x)$ rezultă $\vartheta(x)=$ $=O(x)$.

Înainte de a demonstra şi alte proprietăţi în care intervine $\vartheta(x)$, vom demonstra următoarea teoremă.

Teoremă.

$$\sum_{p\leqslant x}\frac{\log p}{p}=\log x+O(1),$$

suma fiind extinsă la toate numerele prime pozitive, diferite două cîte două, cel mult egale cu un număr real x.

Demonstraţie. Avem $\sum_{1\leqslant n\leqslant x}\frac{\Lambda(n)}{n}=\log x+O(1)$ şi $\sum_{1\leqslant n\leqslant x}\frac{\Lambda(n)}{n}=$

$$=\sum_{p\leqslant x}\frac{\log p}{p}+\left(\sum_{p^2\leqslant x}\frac{\log p}{p^2}+\sum_{p^3\leqslant x}\frac{\log p}{p^3}+\ldots\right),$$

deoarece funcţia lui Mangoldt este egală cu zero dacă numărul natural n nu este o putere, cu exponent număr natural, a unui număr prim şi este egală cu logaritmul unui număr prim pozitiv dacă numărul natural n este o putere, cu exponent număr natural, a numărului prim considerat. Sumele din paranteză, care sînt de forma

$$\sum_{p^r\leqslant x}\frac{\log p}{p^r},$$

sînt extinse la toate numerele prime pozitive p, diferite două cîte două, care satisfac relația $p^r \leqslant x$, r fiind un număr natural, același pentru toate numerele prime considerate. Avem

$$\sum_{p^r \leqslant x} \frac{\log p}{p^r} = \sum_{p \leqslant x^{1/r}} \frac{\log p}{p^r},$$

deoarece relațiile $p^r \leqslant x$ și $p \leqslant x^{1/r}$ sînt echivalente în condițiile de mai sus. Deci

$$\left| \sum_{p^2 \leqslant x} \frac{\log p}{p^2} + \sum_{p^3 \leqslant x} \frac{\log p}{p^3} + \dots \right| = \sum_{p \leqslant x^{1/2}} \frac{\log p}{p^2} + \sum_{p \leqslant x^{1/3}} \frac{\log p}{p^3} + \dots \leqslant$$

$$\leqslant \sum_{p \leqslant x} \frac{\log p}{p^2} + \sum_{p \leqslant x} \frac{\log p}{p^3} + \dots = \sum_{p \leqslant x} \log p \left(\frac{1}{p^2} + \frac{1}{p^3} + \dots \right) \leqslant$$

$$\leqslant \sum_{p \leqslant x} \log p \sum_{s=2}^{\infty} \frac{1}{p^s} = \sum_{p \leqslant x} \frac{\log p}{p(p-1)} \leqslant 2 \sum_{p \leqslant x} p^{-2} \log p \leqslant 2 \sum_{1 \leqslant n \leqslant x} n^{-2} \log n,$$

deoarece pentru $p \geqslant 2$ avem $p - 1 \geqslant \frac{1}{2} p$, ceea ce se stabilește scriind pe $p \geqslant 2$ sub forma $2p \geqslant 2 + p$, deci $2(p-1) \geqslant p$, deci $p - 1 \geqslant \frac{1}{2} p$. Așadar,

$$\sum_{p^2 \leqslant x} \frac{\log p}{p^2} + \sum_{p^3 \leqslant x} \frac{\log p}{p^3} + \dots = O(1),$$

avînd $\sum_{1 \leqslant n \leqslant x} n^{-2} \log n = O(1)$ și deci relația din enunțul teoremei este demonstrată.

(5) *Există un număr real a care verifică inegalitățile $0 < a < 1$ astfel încît $\vartheta(x) > ax$ pentru orice x pentru care $x \geqslant 2$.*

Demonstrație. Dacă c este un număr real care verifică inegalitățile $0 < c < 1$ atunci

$$\frac{\vartheta(x)}{cx} = \frac{1}{cx} \sum_{p \leqslant x} \log p \geqslant \frac{1}{cx} \sum_{cx < p \leqslant x} \log p > \sum_{cx < p \leqslant x} \frac{\log p}{p} =$$

$$= \sum_{p \leqslant x} \frac{\log p}{p} - \sum_{p \leqslant cx} \frac{\log p}{p}.$$

Dar, după teorema demonstrată mai sus,

$$\sum_{p \leqslant x} \frac{\log p}{p} = \log x + h(x),$$

unde $h(x) = O(1)$, adică există două constante pozitive C_1 și C_2 astfel încît pentru orice x pentru care $x > C_2$ să avem $|O(1)| < C_1$. Deci

$$\sum_{p \leqslant cx} \frac{\log p}{p} = \log cx + h(cx),$$

unde cu aceleași constante pozitive C_1 și C_2 avem $|h(cx)| < C_1$ pentru orice x pentru care $cx > C_2$. Deoarece $0 < c < 1$, pentru orice x pentru care $x > \frac{C_2}{c}$ avem

$$|h(x) - h(cx)| \leqslant |h(x)| + |h(cx)| < 2C_1.$$

Deci

$$\frac{\vartheta(x)}{cx} > \log x + h(x) - (\log cx + h(cx)) = \log \frac{1}{c} + (h(x) - h(cx)),$$

și există două constante pozitive C și C_2 astfel încît pentru orice x pentru care $x > \frac{C_2}{c}$ să avem

$$-C < h(x) - h(cx) < C,$$

unde am pus $C = 2C_1$. Dar atunci

$$-1 + \log \frac{1}{c} - C < -1 + \log \frac{1}{c} + (h(x) - h(cx))$$

pentru orice x pentru care $x > \frac{C_2}{c}$. Putem alege pe c astfel încît să avem

$$0 < -1 + \log \frac{1}{c} - C,$$

deoarece este suficient să luăm $c < e^{-1-C}$. Dar atunci

$$0 < -1 + \log \frac{1}{c} + (h(x) - h(cx))$$

pentru orice x pentru care $x>\frac{C_2}{c}$, deci

$$\frac{\vartheta(x)}{cx}>1$$

pentru orice x pentru care $x>\frac{C_2}{c}$ sau

$$\frac{\vartheta(x)}{x}>c$$

pentru orice x pentru care $x>\frac{C_2}{c}$. Pentru orice x din intervalul $\left[2, \frac{C_2}{c}\right]$ valoarea lui $\frac{\vartheta(x)}{x}$ este diferită de 0, ceea ce rezultă din definiția lui $\vartheta(x)$. Dacă notăm cu b cea mai mică valoare a lui $\frac{\vartheta(x)}{x}$ în intervalul $\left[2,\frac{C_2}{c}\right]$ avem $b>0$. Dacă luăm un număr real a astfel încît $0<a<\min(b, c)$, atunci

$$\frac{\vartheta(x)}{x}>a$$

pentru orice x pentru care $x\geqslant 2$, avînd $0<a<1$. Din aceasta obținem demonstrația proprietății (5).

(6) $$\sum_{1\leqslant n\leqslant x}\frac{\vartheta(n)}{n^2}=\log x+O(1).$$

Demonstrație. Pornim de la relația

$$\sum_{p\leqslant x}\frac{\log p}{p}=\log x+O(1).$$

Dar $\sum_{p\leqslant x}\frac{\log p}{p}=\sum_{1\leqslant n\leqslant x}\frac{\vartheta(n)-\vartheta(n-1)}{n}$, ultima sumă fiind extinsă la toate numerele naturale, diferite două cîte două, cel mult egale cu x, deoarece $\vartheta(n)-\vartheta(n-1)=\sum_{p\leqslant n}\log p-\sum_{p\leqslant n-1}\log p=\log n$

dacă n este prim și $\vartheta(n)-\vartheta(n-1)=0$ dacă n nu este prim. Avem

$$\sum_{1\leqslant n\leqslant x}\frac{\vartheta(n)-\vartheta(n-1)}{n}=\sum_{1\leqslant n\leqslant x}\frac{\vartheta(n)}{n}-\sum_{1\leqslant n\leqslant x}\frac{\vartheta(n-1)}{n}=$$

$$=\sum_{1\leqslant n\leqslant x}\frac{\vartheta(n)}{n}-\sum_{0\leqslant n\leqslant x-1}\frac{\vartheta(n)}{n+1}=\sum_{1\leqslant n\leqslant x}\frac{\vartheta(n)}{n}-\sum_{1\leqslant n\leqslant x}\frac{\vartheta(n)}{n+1}-$$

$$-\frac{\vartheta(0)}{0+1}+\frac{\vartheta([x])}{[x]+1}=\sum_{1\leqslant n\leqslant x}\frac{\vartheta(n)}{n(n+1)}+\frac{\vartheta(x)}{[x]+1}=\sum_{1\leqslant n\leqslant x}\frac{\vartheta(n)}{n^2}+$$

$$+\sum_{1\leqslant n\leqslant x}\vartheta(n)\left(\frac{1}{n(n+1)}-\frac{1}{n^2}\right)+\frac{\vartheta(x)}{[x]+1}.$$

Mai departe

$$\sum_{1\leqslant n\leqslant x}\vartheta(n)\left(\frac{1}{n(n+1)}-\frac{1}{n^2}\right)=-\sum_{1\leqslant n\leqslant x}\frac{\vartheta(n)}{n^2(n+1)}=$$

$$=-\sum_{1\leqslant n\leqslant x}\frac{O(n)}{n^2(n+1)}=-O\left(\sum_{1\leqslant n\leqslant x}\frac{1}{n(n+1)}\right)=$$

$$=O\left(\sum_{1\leqslant n\leqslant x}\left(\frac{1}{n}-\frac{1}{n+1}\right)\right)=O\left(1-\frac{1}{[x]+1}\right)=O(O(1))=O(1).$$

Am putut scrie

$$\sum_{1\leqslant n\leqslant x}\frac{O(n)}{n^2(n+1)}=O\left(\sum_{1\leqslant n\leqslant x}\frac{n}{n^2(n+1)}\right),$$

deoarece funcțiile $\frac{1}{x^2(x+1)}$, x și $O(x)$ sînt definite pentru orice număr natural x, iar $\frac{x}{x^2(x+1)}\neq 0$ măcar pentru un număr natural a.

Din cauză că

$$\frac{\vartheta(x)}{[x]+1}=\frac{O(x)}{[x]+1}=O\left(\frac{x}{[x]+1}\right)=O(O(1))=O(1),$$

rezultă din cele de mai sus că

$$\log x+O(1)=\sum_{1\leqslant n\leqslant x}\frac{\vartheta(n)}{n^2}+O(1)+O(1),$$

deci proprietatea (6) este demonstrată.

(7) $$\sum_{1\leqslant n\leqslant x}\frac{\Psi(n)}{n^2}=\log x+O(1).$$

Demonstrație. După proprietatea (2) avem $\Psi(x)=\vartheta(x)+$ $+O(x^{1/2}\log^2 x)$, deci

$$\sum_{1\leqslant n\leqslant x}\frac{\Psi(n)}{n^2}=\sum_{1\leqslant n\leqslant x}\frac{\vartheta(n)+O(n^{1/2}\log^2 n)}{n^2}=\sum_{1\leqslant n\leqslant x}\frac{\vartheta(n)}{n^2}+$$

$$+\sum_{1\leqslant n\leqslant x}\frac{O(n^{1/2}\log^2 n)}{n^2}=\log x+O(1)+O\left(\sum_{1\leqslant n\leqslant x}\frac{n^{1/2}\log^2 n}{n^2}\right).$$

Am putut scrie

$$\sum_{1\leqslant n\leqslant x}\frac{O(n^{1/2}\log^2 n)}{n^2}=O\left(\sum_{1\leqslant n\leqslant x}\frac{n^{1/2}\log^2 n}{n^2}\right),$$

deoarece funcțiile $\frac{1}{x^2}$, $x^{1/2}\log^2 x$, $O(x^{1/2}\log^2 x)$ sînt definite pentru orice număr natural x, iar $\frac{x^{1/2}\log^2 x}{x^2}\neq 0$ măcar pentru un număr natural a. Însă

$$\sum_{1\leqslant n\leqslant x}\frac{n^{1/2}\log^2 n}{n^2}=\sum_{1\leqslant n\leqslant x}n^{-3/2}\log^2 n=O(1)$$

și deci proprietatea (7) este demonstrată.

Capitolul 15

LEGEA ASIMPTOTICĂ A DISTRIBUȚIEI NUMERELOR PRIME

15.1. Funcția $R(x)$

Definiție. *Funcția $R(x)$ este definită prin*

$$\Psi(x)=x+R(x).$$

Proprietăți ale funcției $R(x)$:

(1) $$|R(x)|\log x\leqslant\sum_{1\leqslant n\leqslant x}\left|R\left(\frac{x}{n}\right)\right|\Lambda(n)+o(x\log x).$$

Demonstrație. În relația lui Selberg

$$\Psi(x)\log x+\sum_{1\leqslant n\leqslant x}\Psi\left(\frac{x}{n}\right)\Lambda(n)=2x\log x+O(x)$$

punînd $\Psi(x)=x+R(x)$ obținem

$$(x+R(x))\log x+\sum_{1\leqslant n\leqslant x}\left(\frac{x}{n}+R\left(\frac{x}{n}\right)\right)\Lambda(n)=2x\log x+O(x).$$

Însă

$$(x+R(x))\log x+\sum_{1\leqslant n\leqslant x}\left(\frac{x}{n}+R\left(\frac{x}{n}\right)\right)\Lambda(n)=x\log x+R(x)\log x+$$

$$+x\sum_{1\leqslant n\leqslant x}\frac{\Lambda(n)}{n}+\sum_{1\leqslant n\leqslant x}R\left(\frac{x}{n}\right)\Lambda(n)=x\log x+R(x)\log x+x(\log x+$$

$$+O(1))+\sum_{1\leqslant n\leqslant x}R\left(\frac{x}{n}\right)\Lambda(n)=2x\log x+R(x)\log x+O(x)+$$

$$+\sum_{1\leqslant n\leqslant x}R\left(\frac{x}{n}\right)\Lambda(n).$$

Deci

$$R(x)\log x+\sum_{1\leqslant n\leqslant x}R\left(\frac{x}{n}\right)\Lambda(n)=O(o(x\log x))$$

sau

$$R(x)\log x=-\sum_{1\leqslant n\leqslant x}R\left(\frac{x}{n}\right)\Lambda(n)+o(x\log x).$$

Luînd valorile absolute, obținem proprietatea (1).

(2) $|R(x)|\log x\leqslant\sum_{mn\leqslant x}\left|R\left(\frac{x}{mn}\right)\right|\frac{\Lambda(m)\Lambda(n)}{\log mn}+o(x\log x)$.

Demonstrație. În relația (8), din paragraful 14.2,

$$\Psi(x)\log x=\sum_{mn\leqslant x}\frac{\Lambda(m)\Lambda(n)}{\log mn}\Psi\left(\frac{x}{mn}\right)+o(x\log x)$$

punînd $\Psi(x)=x+R(x)$ obținem

$$(x+R(x))\log x=\sum_{mn\leqslant x}\frac{\Lambda(m)\Lambda(n)}{\log mn}\left(\frac{x}{mn}+R\left(\frac{x}{mn}\right)\right)+o(x\log x)=$$

$$=x\sum_{mn\leqslant x}\frac{\Lambda(m)\Lambda(n)}{mn\log mn}+\sum_{mn\leqslant x}\frac{\Lambda(m)\Lambda(n)}{\log mn}R\left(\frac{x}{mn}\right)+o(x\log x)=$$

$$=x(\log x+O(\log\log x))+\sum_{mn\leqslant x}\frac{\Lambda(m)\Lambda(n)}{\log mn}R\left(\frac{x}{mn}\right)+o(x\log x)=$$

$$=x\log x+O(o(x\log x))+\sum_{mn\leqslant x}\frac{\Lambda(m)\Lambda(n)}{\log mn}R\left(\frac{x}{mn}\right)+o(x\log x).$$

Deci

$$R(x)\log x=\sum_{mn\leqslant x}\frac{\Lambda(m)\Lambda(n)}{\log mn}R\left(\frac{x}{mn}\right)+o(x\log x).$$

Luînd valorile absolute, obținem proprietatea (2).

(3) $|R(x)|\leqslant\frac{1}{\log x}\sum_{1\leqslant k\leqslant x}\left|R\left(\frac{x}{k}\right)\right|+o(x)$.

Demonstrație. Adunînd membru cu membru inegalitățile din (1) și (2) obținem

$$2|R(x)|\log x\leqslant\sum_{1\leqslant n\leqslant x}\left|R\left(\frac{x}{n}\right)\right|\Lambda(n)+\sum_{mn\leqslant x}\left|R\left(\frac{x}{mn}\right)\right|\frac{\Lambda(m)\Lambda(n)}{\log mn}+$$

$$+o(x\log x).$$

Cu formula de transformare a sumelor a lui Abel, obținem

$$\sum_{1\leqslant n\leqslant x}\left|R\left(\frac{x}{n}\right)\right|\Lambda(n)=\sum_{n=1}^{[x]}\left|R\left(\frac{x}{n}\right)\right|\Lambda(n)=$$

$$=\sum_{k=1}^{[x]}\left(\sum_{l=1}^{k}\Lambda(l)\right)\left(\left|R\left(\frac{x}{k}\right)\right|-\left|R\left(\frac{x}{k+1}\right)\right|\right)+\left(\sum_{i=1}^{[x]}\Lambda(l)\right)\left|R\left(\frac{x}{[x]+1}\right)\right|.$$

Apoi $0<x<[x]+1$, deci $0<\frac{x}{[x]+1}<1$ și cum $\Psi\left(\frac{x}{[x]+1}\right)=\frac{x}{[x]+1}+R\left(\frac{x}{[x]+1}\right)$ și $\Psi\left(\frac{x}{[x]+1}\right)=0$ ca urmare a faptului că $0<\frac{x}{[x]+1}<1$, avem $\left|R\left(\frac{x}{[x]+1}\right)\right|=\left|\frac{x}{[x]+1}\right|<1$, deci

$$\left|\left(\sum_{l=1}^{[x]}\Lambda(l)\right)\left|R\left(\frac{x}{[x]+1}\right)\right|\right|=\left(\sum_{1\leqslant l\leqslant x}\Lambda(l)\right)\left|R\left(\frac{x}{[x]+1}\right)\right|<\sum_{1\leqslant l\leqslant x}\Lambda(l)=\Psi(x)=$$

$$=O(x)=o(x\ \log\ x),$$

deci

$$\sum_{1\leqslant n\leqslant x}\left|\ R\left(\frac{x}{n}\right)\right|\Lambda(n)=\sum_{1\leqslant k\leqslant x}\left(\sum_{1\leqslant l\leqslant k}\Lambda(l)\right)\left(\left|\ R\left(\frac{x}{k}\right)\right|-\left|R\left(\frac{x}{k+1}\right)\right|\right)+$$

$$+o(x\ \log\ x).$$

Tot cu formula de transformare a sumelor a lui Abel obținem

$$\sum_{mn\leqslant x}\left|\ R\left(\frac{x}{mn}\right)\right|\frac{\Lambda(m)\ \Lambda(n)}{\log\ mn}=\sum_{1\leqslant k\leqslant x}\left|\ R\left(\frac{x}{k}\right)\right|\sum_{n|k}\frac{\Lambda\left(\frac{k}{n}\right)\Lambda(n)}{\log\ k}=$$

$$=\sum_{k=1}^{[x]}\left|\ R\left(\frac{x}{k}\right)\right|\sum_{n|k}\frac{\Lambda\left(\frac{k}{n}\right)\Lambda(n)}{\log\ k}=$$

$$=\sum_{k=1}^{[x]}\left(\sum_{l=1}^{k}\sum_{n|l}\frac{\Lambda\left(\frac{l}{n}\right)\Lambda(n)}{\log\ l}\right)\left(\left|\ R\left(\frac{x}{k}\right)\right|-\left|\ R\left(\frac{x}{k+1}\right)\right|\right)+$$

$$+\sum_{l=1}^{[x]}\left(\sum_{n|l}\frac{\Lambda\left(\frac{l}{n}\right)\Lambda(n)}{\log\ l}\right)\left|\ R\left(\frac{x}{[x]+1}\right)\right|=$$

$$=\sum_{1\leqslant k\leqslant x}\left(\sum_{1\leqslant l\leqslant k}\sum_{n|l}\frac{\Lambda\left(\frac{l}{n}\right)\Lambda(n)}{\log\ l}\right)\left(\left|\ R\left(\frac{x}{k}\right)\right|-\left|\ R\left(\frac{x}{k+1}\right)\right|\right)+$$

$$+\sum_{1\leqslant l\leqslant x}\left(\sum_{n|l}\frac{\Lambda\left(\frac{l}{n}\right)\Lambda(n)}{\log\ l}\right)\left|\ R\left(\frac{x}{[x]+1}\right)\right|=$$

$$=\sum_{1\leqslant k\leqslant x}\left(\sum_{mn\leqslant k}\frac{\Lambda(m)\ \Lambda(n)}{\log\ mn}\right)\left(\left|\ R\left(\frac{x}{k}\right)\right|-\left|\ R\left(\frac{x}{k+1}\right)\right|\right)+$$

$$+\sum_{mn\leqslant x}\frac{\Lambda(m)\ \Lambda(n)}{\log\ mn}\left|\ R\left(\frac{x}{[x]+1}\right)\right|.$$

Avem $\left|\sum_{mn\leqslant x}\frac{\Lambda(m)\ \Lambda(n)}{\log\ mn}\ R\left(\frac{x}{[x]+1}\right)\right|<$

$$<\sum_{mn\leqslant x}\frac{\Lambda(m)\ \Lambda(n)}{\log\ mn}=2x-\Psi(x)+o(x)=o(x\ \log\ x).$$

Deci

$$\sum_{mn\leqslant x}\left|\ R\left(\frac{x}{mn}\right)\right|\frac{\Lambda(m)\ \Lambda(n)}{\log\ mn}=\sum_{\leqslant k\leqslant x}\left(\sum_{mn\leqslant k}\frac{\Lambda(m)\ \Lambda(n)}{\log\ mn}\right)\left(\left|\ R\left(\frac{x}{k}\right)\right|-\right.$$

$$\left.-\left|\ R\left(\frac{x}{k+1}\right)\right|\right)+o(x\ \log\ x).$$

Obținem deci

$$2|R(x)|\log x\leqslant\sum_{1\leqslant k\leqslant x}\left(\sum_{1\leqslant l\leqslant k}\Lambda(l)+\sum_{mn\leqslant k}\frac{\Lambda(m)\ \Lambda(n)}{\log\ mn}\right)\left(\left|\ R\left(\frac{x}{k}\right)\right|-\right.$$

$$\left.-\left|R\left(\frac{x}{k+1}\right)\right|\right)+o\ (x\ \log\ x)=\sum_{1\leqslant k\leqslant x}(2k+o(k))\left(\left|R\left(\frac{x}{k}\right)\right|-\left|R\left(\frac{x}{k+1}\right)\right|\right)+$$

$$+o(x\log x),$$

deoarece am utilizat relația (6) din paragraful 14.2. Avem

$$\sum_{1\leqslant k\leqslant x}k\left(\left|R\left(\frac{x}{k}\right)\right|-\left|\ R\left(\frac{x}{k+1}\right)\right|\right)=\left(\left|\ R\left(\frac{x}{1}\right)\right|-\left|R\left(\frac{x}{2}\right)\right|\right)+$$

$$+2\left(\left|\ R\left(\frac{x}{2}\right)\right|-\left|\ R\left(\frac{x}{3}\right)\right|\right)+\ldots+[x]\left(\left|\ R\left(\frac{x}{[x]}\right)\right|-\left|\ R\left(\frac{x}{[x]+1}\right)\right|\right)=$$

$$=\sum_{1\leqslant k\leqslant x}\left|R\left(\frac{x}{k}\right)\right|-[x]\left|\ R\left(\frac{x}{[x]+1}\right)\right|=\sum_{1\leqslant k\leqslant x}\left|\ R\left(\frac{x}{k}\right)\right|+o(x\ \log\ x),$$

deoarece $\left|-[x]\left|R\left(\frac{x}{[x]+1}\right)\right|\right|<[x]\leqslant x=o(x\log x)$, deci $-\lfloor x\rfloor\left|R\left(\frac{x}{[x]+1}\right)\right|=$

$=o(x\ \log\ x)$. Apoi

$$\sum_{1\leqslant k\leqslant x}o(k)\left(\left|R\left(\frac{x}{k}\right)\right|-\left|\ R\left(\frac{x}{k+1}\right)\right|\right)=\sum_{1\leqslant k\leqslant C_2}o(k)\left(\left|R\left(\frac{x}{k}\right)\right|-\left|\ R\left(\frac{x}{k+1}\right)\right|\right)+$$

$$+\sum_{C_2<k\leqslant x}o(k)\left(\left|\ R\left(\frac{x}{k}\right)\right|-\left|R\left(\frac{x}{k+1}\right)\right|\right),$$

unde C_2 este o constantă care există atunci cînd este dat un număr real ε pozitiv astfel încît să avem

$$|o(k)|<\varepsilon k$$

îndată ce $k>C_2$. Deci

$$\left|\sum_{C_2<k\leqslant x} o(k)\left(\left|R\left(\frac{x}{k}\right)\right|-\left|R\left(\frac{x}{k+1}\right)\right|\right)\right|\leqslant \sum_{C_2<k\leqslant x}\left|o(k)\right|\left|\left|R\left(\frac{x}{k}\right)\right|-\left|R\left(\frac{x}{k+1}\right)\right|\right|<$$

$$<\varepsilon\sum_{C_2<k\leqslant x} k\left|R\left(\frac{x}{k}\right)-R\left(\frac{x}{k+1}\right)\right|\leqslant \varepsilon\sum_{C_2<k\leqslant x} k\left(\left|\Psi\left(\frac{x}{k}\right)-\Psi\left(\frac{x}{k+1}\right)\right|+\right.$$

$$\left.+\left|\frac{x}{k}-\frac{x}{k+1}\right|\right)=\varepsilon\sum_{C_2<k\leqslant x} k\left(\Psi\left(\frac{x}{k}\right)-\Psi\left(\frac{x}{k+1}\right)+\frac{x}{k(k+1)}\right)\leqslant$$

$$\leqslant\varepsilon\sum_{1\leqslant k\leqslant x} k\left(\Psi\left(\frac{x}{k}\right)-\Psi\left(\frac{x}{k+1}\right)+\frac{x}{k(k+1)}\right)=$$

$$=\varepsilon\left(\sum_{1\leqslant k\leqslant x}\Psi\left(\frac{x}{k}\right)+x\sum_{1\leqslant k\leqslant x}\frac{1}{k+1}-[x]\Psi\left(\frac{x}{[x]+1}\right)\right)=$$

$$=\varepsilon\left(\sum_{1\leqslant k\leqslant x} O\left(\frac{x}{k}\right)+x\sum_{2\leqslant k\leqslant x+1}\frac{1}{k}\right)=\varepsilon\left(O\left(x\sum_{1\leqslant k\leqslant x}\frac{1}{k}\right)+x\sum_{2\leqslant k\leqslant x+1}\frac{1}{k}\right)=$$

$$=\varepsilon\left(O\left(x\left(\log x+C_1+O\left(\frac{1}{x}\right)\right)\right)+x\left(\log(x+1)+C_3+O\left(\frac{1}{x+1}\right)\right)\right)=$$

$$=\varepsilon O(x\log x).$$

Pe parcurs am utilizat faptul că $\left|\left|R\left(\frac{x}{k}\right)\right|-\left|R\left(\frac{x}{k+1}\right)\right|\right|\leqslant$ $\leqslant\left|R\left(\frac{x}{k}\right)-R\left(\frac{x}{k+1}\right)\right|$, $\Psi(x)=x+R(x)$, $\Psi\left(\frac{x}{[x]+1}\right)=0$, $\Psi(x)=$ $=O(x)$, $\Psi\left(\frac{x}{k+1}\right)\leqslant\Psi\left(\frac{x}{k}\right)$. Deci fiind dat ε real pozitiv avem

$$\left|\frac{\sum_{C_2<k\leqslant x} o(k)\left(\left|R\left(\frac{x}{k}\right)\right|-\left|R\left(\frac{x}{k+1}\right)\right|\right)}{O(x\log x)}-0\right|<\varepsilon$$

pentru orice x pentru care $x>1$, deci

$$\sum_{C_2<k\leqslant x}\frac{o(k)}{}\left(\left|R\left(\frac{x}{k}\right)\right|-\left|R\left(\frac{x}{k+1}\right)\right|\right)=o(O(x\log x))=o(x\log x).$$

Apoi avem

$$\sum_{1\leqslant k\leqslant C_2}\frac{o(k)}{}\left(\left|R\left(\frac{x}{k}\right)\right|-\left|R\left(\frac{x}{k+1}\right)\right|\right)=\sum_{1\leqslant k\leqslant C_2} o(k)O(x)=$$

$$=O(x)=O(o(x\log x))=o(x\log x),$$

deoarece aici avem un număr finit de termeni. Deci

$$\sum_{1\leqslant k\leqslant x}\frac{o(k)}{}\left(\left|R\left(\frac{x}{k}\right)\right|-\left|R\left(\frac{x}{k+1}\right)\right|\right)=o(x\log x).$$

Am demonstrat deci că

$$2\,|R(x)|\log x\leqslant 2\left(\sum_{1\leqslant k\leqslant x}\left|R\left(\frac{x}{k}\right)\right|+o(x\log x)\right)+o(x\log x),$$

de unde prin împărțire cu $2\log x$ rezultă proprietatea (3).

(4) *Dacă* $x'\triangleright x$ *atunci* $|R(x)-R(x')|\leqslant x'-x+o(x')$.

Demonstrație. Avem $\psi(x)=x+R(x)$, $\psi(x')=x'+R(x')$ deci $\psi(x')-\psi(x)=x'-x+R(x')-R(x)$. Din cauză că $x'\triangleright x$ avem $\psi(x')\geqslant$ $\geqslant\psi(x)$ sau $\psi(x')-\psi(x)\geqslant 0$ deci $x'-x+R(x')-R(x)\geqslant 0$. Dacă $R(x')-R(x)<0$ avem $x'-x\geqslant-(R(x')-R(x))=|R(x')-R(x)|$ și proprietatea este demonstrată. Dacă $R(x')-R(x)\geqslant 0$ avem $\sum_{mn\leqslant x}\frac{\Lambda(m)\,\Lambda(n)}{\log mn}=2x-\Psi(x)+o(x)$ și $\sum_{mn\leqslant x'}\frac{\Lambda(m)\,\Lambda(n)}{\log mn}=2x'-\Psi(x')+$ $+o(x')$, deci $\sum_{mn\leqslant x'}\frac{\Lambda(m)\,\Lambda(n)}{\log mn}-\sum_{mn\leqslant x}\frac{\Lambda(m)\,\Lambda(n)}{\log mn}=2x'-2x-\Psi(x')+$ $+\Psi(x)+o(x')-o(x)$. Din cauză că $x'\triangleright x$ avem $\sum_{mn\leqslant x'}\frac{\Lambda(m)\,\Lambda(n)}{\log mn}-$ $-\sum_{mn\leqslant x}\frac{\Lambda(m)\,\Lambda(n)}{\log mn}\geqslant 0$, deci $0\leqslant 2x'-2x-\Psi(x')+\Psi(x)+o(x')-o(x)$.

Ținînd seama de $\Psi(x')=x'+R(x')$, $\Psi(x)=x+R(x)$ se deduce $R(x')-R(x)\leqslant x'-x+o(x')-o(x)$. Însă $R(x')-R(x)=|R(x')-R(x)|$, deoarece am presupus că $R(x')-R(x)\geqslant 0$. Apoi $o(x)=o(O(x'))=o(x')$, deci proprietatea (4) este complet demonstrată.

(5) *Dacă δ este un număr real care satisface inegalitățile $0<\delta<1$, atunci există două numere reale $\rho(\delta)$ și $x_0=x_0(\delta)$, unde $\rho(\delta)>1$, astfel încît pentru orice x pentru care $x\geqslant x_0$ să existe în intervalul $[x,\ \rho x]$, unde $\rho\geqslant\rho(\delta)$, un y cu proprietatea $|R(y)|<\delta y$.*

Demonstrație. Mai întîi ne vom folosi de relația

$$\sum_{1\leqslant n\leqslant x}\frac{\Psi(n)}{n^2}=\log x+O(1),$$

în care punînd $\Psi(n)=n+R(n)$ obținem

$$\log x+O(1)=\sum_{1\leqslant n\leqslant x}\frac{\Psi(n)}{n^2}=\sum_{1\leqslant n\leqslant x}\frac{n+R(n)}{n^2}=\sum_{1\leqslant n\leqslant x}\frac{1}{n}+$$

$$+\sum_{1\leqslant n\leqslant x}\frac{R(n)}{n^2}=\log x+C+O\left(\frac{1}{x}\right)+\sum_{1\leqslant n\leqslant x}\frac{R(n)}{n^2}.$$

Deci

$$\sum_{1\leqslant n\leqslant x}\frac{R(n)}{n^2}=O(1),$$

deoarece $C=O(1)$ și $\frac{1}{x}=O(1)$. Pentru orice număr real $\rho>1$ avem

$$\sum_{x<n\leqslant\rho x}\frac{R(n)}{n^2}=\sum_{1\leqslant n\leqslant\rho x}\frac{R(n)}{n^2}-\sum_{1\leqslant n\leqslant x}\frac{R(n)}{n^2}=O(1)-O(1)=O(1).$$

Există deci două constante pozitive C_1 și C_2 astfel încît

$$\left|\sum_{x<n\leqslant\rho x}\frac{R(n)}{n^2}\right|<C_1$$

pentru orice x pentru care $x\geqslant C_2$.

Dacă pentru valorile lui n care verifică inegalitățile $x<n\leqslant\rho x$, valorile lui $R(n)$ au același semn, putînd avea și $R(n)=0$ pentru unele valori ale lui n, avem dreptul să scriem

$$\left|\sum_{x<n\leqslant\rho x}\frac{R(n)}{n^2}\right|=\sum_{x<n\leqslant\rho x}\frac{|R(n)|}{n^2}\geqslant\left(\sum_{x<n\leqslant\rho x}\frac{1}{n}\right)\frac{|R(y)|}{y},$$

unde y este acea valoare din intervalul $[x,\ \rho x]$ pentru care funcția $\frac{|R(u)|}{u}$ își atinge minimul. Așadar

$$|R(y)|<\frac{C_1}{\sum_{x<n\leqslant\rho x}\frac{1}{n}}\,y$$

pentru orice x pentru care $x>C_2$. Însă

$$\sum_{x<n\leqslant\rho x}\frac{1}{n}=\sum_{1\leqslant n\leqslant\rho x}\frac{1}{n}-\sum_{1\leqslant n\leqslant x}\frac{1}{n}=\log\rho x+C+O\left(\frac{1}{\rho x}\right)-\log x-C-O\left(\frac{1}{x}\right)=$$

$$=\log\rho+O\left(\frac{1}{x}\right).$$

Există două constante pozitive C_3 și C_4 astfel încît

$$\left|O\left(\frac{1}{x}\right)\right|<C_3\frac{1}{x}$$

pentru orice x pentru care $x>C_4$. Deci

$$-\frac{C_3}{x}<O\left(\frac{1}{x}\right)<\frac{C_3}{x}$$

pentru orice x pentru care $x>C_4$. Rezultă

$$\frac{1}{2}\log\rho-\frac{C_3}{x}<\frac{1}{2}\log\rho+O\left(\frac{1}{x}\right)$$

pentru orice x pentru care $x>C_4$. Dacă $x>\frac{2C_3}{\log\rho}$ avem $0<$

$<\frac{1}{2}\log\rho-\frac{C_3}{x}$, deci dacă $x>\max\left(C_4,\ \frac{2C_3}{\log\rho}\right)$ avem

$$\sum_{x<n\leqslant\rho x}\frac{1}{n}=\frac{1}{2}\log\rho+\left(\frac{1}{2}\log\rho+O\left(\frac{1}{x}\right)\right)>\frac{1}{2}\log\rho.$$

În consecință pentru orice $x > \max\left(C_2,\ C_4, \frac{2C_3}{\log \rho}\right)$ avem

$$|R(y)| < \frac{2C_1}{\log \rho} y.$$

Dacă luăm $\rho \geqslant \rho(\delta) = e^{\frac{2C_1}{\delta}}$, din faptul că $0<\delta$ obținem $\rho(\delta)>1$, avînd în vedere că $\frac{2C_1}{\delta}>0$, și apoi

$$|R(y)| < \delta y$$

pentru orice $x > \max(C_2,\ C_4, \frac{2C_3}{\log \rho})$, atunci cînd pentru valorile lui n care verifică inegalitățile $x<n\leqslant \rho x$ valorile lui $R(n)$ au același semn. Se mai constată că y se află în intervalul $[x,\ \rho x]$.

Dacă pentru valorile lui n care verifică inegalitățile $x<n\leqslant \rho x$ există valori $R(n)$ cu semne diferite, atunci există y în intervalul $[x,\ \rho x]$ astfel încît $R(y)$ și $R(y+1)$ să aibă semne diferite sau unul din ele să fie zero. Avem de considerat două cazuri :

(a) $R(y)\geqslant 0$, $R(y+1)<0$. Ținînd seama de $\Psi(y)\leqslant\Psi(y+1)$ obținem $R(y)=\Psi(y)-y\leqslant \Psi(y+1)-y=\Psi(y+1)-(y+1)+1=$ $=R(y+1)+1$ deci $R(y)<1$ și cum $R(y)\geqslant 0$ avem $|R(y)|<1$.

(b) $R(y)\leqslant 0$, $R(y+1)>0$. Din $R(y+1)>0$ rezultă $\Psi(y+1)>$ $>y+1$, iar din $R(y)\leqslant 0$ rezultă $\Psi(y)\leqslant y$, deci $\Psi(y+1)\geqslant y+1\geqslant$ $\geqslant \Psi(y)+1$. Rezultă că $\Psi(y+1)-\Psi(y)\geqslant 1$. Din $\Psi(y+1)>\Psi(y)$ rezultă că $\Psi(y+1)=\sum\limits_{1\leqslant n\leqslant y+1}\Lambda(n)=\sum\limits_{1\leqslant n\leqslant y}\Lambda(n)+\Lambda([y]+1)$. Așadar $[y]+1=p_r$, unde p este un număr prim pozitiv, iar r un număr natural. Obținem $0<R(y+1)=\Psi(y+1)-(y+1)=\Psi(y)+\log p-$ $-(y+1)=R(y)+\log p-1$, deci $|R(y)|=-R(y)<\log p-1=$ $=\frac{\log([y]+1)}{r}-1<\log(y+1)-1$.

Pentru a evalua în continuare, să considerăm funcția

$$f(u)=\log(u+1)-1-\delta u.$$

Avem $f'(u)=\frac{1}{u+1}-\delta$. De aici rezultă că pentru $\frac{1}{u+1}-\delta<0$ sau $\frac{1}{\delta}-1<u$ avem $f'(u)<0$. Am considerat numai valori pozitive ale

lui u ca să obținem $\frac{1}{\delta}-1<u$ din $\frac{1}{u+1}-\delta<0$. Deci funcția $f(u)$ este descrescătoare pentru valorile lui u pentru care $u\geqslant \frac{1}{\delta}-1$. Avem $\lim\limits_{u\to\infty} f(u)=\lim\limits_{u\to\infty}(\log(u+1)-1-\delta u)=\lim\limits_{u\to\infty} u\left(\frac{\log(u+1)}{u}-\delta\right)-1=$ $=\lim\limits_{u\to\infty} u \lim\limits_{u\to\infty}\left(\frac{\log(u+1)}{u}-\delta\right)-1=-\delta\lim\limits_{u\to\infty} u-1=-\infty$. Deci există o constantă pozitivă C_6 astfel încît pentru orice u pentru care $u\geqslant C_6$ să avem $f(u)<0$, funcția $f(u)$ fiind continuă, deci

$$\log(u+1)-1<\delta u$$

pentru orice u pentru care $u>C_6$. Deoarece $x\leqslant y$ rezultă că

$$\log(y+1)-1<\delta y$$

pentru orice x pentru care $x>C_6$.

Deci pentru orice x, pentru care $x>\max\left(C_6, \frac{1}{\delta}\right)$, avem

$$|R(y)|<\delta y,$$

unde y se află în intervalul $[x,\ \rho x]$, deoarece pentru cazul (a) avem $\frac{1}{\delta}<x\leqslant y$, deci $1<\delta y$, iar în cazul (b) avem $\log(y+1)-1<\delta y$ aceasta în cazul cînd pentru valorile lui n care verifică inegalitățile $x<n\leqslant \rho x$ există valori $R(n)$ cu semne diferite. Deci putem lua $x_0=\max\left(C_2,\ C_4,\ \frac{2C_3}{\log\rho},\ C_6,\ \frac{1}{\delta}\right)$.

(6) *Dacă δ este un număr real care satisface inegalitățile $0<\delta<1$, atunci există un număr real $x_1=x_1(\delta)$ pentru care $x_1\geqslant x_0$, astfel încît pentru orice $x>x_1$ și pentru orice z care aparține intersecției intervalelor $[x,\ \rho x]$ și $[y,\ e^{\delta/2}y]$ să avem $|R(z)|<3\delta z$. Numerele reale x_0, ρ și y sînt cele determinate în proprietatea* (5).

Demonstrație. Datorită proprietății (4), pentru $z>y$ avem

$$|R(z)-R(y)|\leqslant z-y+o(z).$$

Aceasta este adevărat şi pentru $z=y$, ceea ce se verifică direct. Obţinem deci

$$|R(z)|=|R(z)-R(y)+R(y)|\leqslant|R(z)-R(y)|+|R(y)|\leqslant|R(y)|+$$
$$+z-y+o(z).$$

Pentru orice număr real şi pozitiv ε există o constantă C astfel încît

$$|o(z)|<\varepsilon z$$

pentru orice z pentru care $z\geqslant C$. Vom lua $\varepsilon=0{,}5\,\delta$ şi $x_1=\max(C,x_0)$. Atunci pentru orice x pentru care $x\geqslant x_1$ vom avea $z\geqslant x>x_1\geqslant C$, deci

$$|o(z)|<0{,}5\delta z\leqslant 0{,}5\delta e^{\delta/2}\,y$$

şi $|R(y)|<\delta y$, deoarece $x_0\leqslant x_1<x$. Deci avem

$$|R(z)|\leqslant|R(y)|+z-y+o(z)\leqslant|R(y)|+z-y+|o(z)|<\delta y+e^{\delta/2}y-$$
$$-y+0{,}5\delta\ e^{\delta/2}y=(\delta-1+e^{\delta/2}(1+0{,}5\delta))y<3\delta z$$

pentru orice $x>x_1$. Ultima inegalitate rezultă din aceea că $y\leqslant z$ şi $(1-u)e^u<1$ pentru $0<u<1$. În adevăr, $f(u)=(1-u)e^u$ ne dă $f'(u)=-e^u+(1-u)e^u=-ue^u$, deci $f'(u)<0$. Funcţia $f(u)$ este descrescătoare în intervalul $[0,\ 1]$, deci $f(0)>f(u)$ cu $0<u<1$ şi cum $f(0)=1$, obţinem $(1-u)e^u<1$. Avem deci $e^{\delta/2}\ (1-0{,}5\ \delta)<1$, de unde $e^{\delta/2}\ (1+0{,}5\ \delta)<\frac{1+0{,}5\delta}{1-0{,}5\delta}=\frac{1-0{,}5\delta+\delta}{1-0{,}5\delta}=1+\frac{\delta}{1-0{,}5\delta}<$ $<1+2\delta$. Evaluarea $\frac{\delta}{1-0{,}5\delta}<2\delta$ este echivalentă cu $1<2-\delta$, adică $\delta<1$, ceea ce am presupus că are loc. Cu aceasta proprietatea (6) a fost demonstrată.

Înainte de a demonstra şi alte proprietăţi în care intervine $R(x)$, vom demonstra :

Teorema lui Cebîşev. *Pentru orice x, pentru care $x\geqslant 2$, există două constante pozitive α şi β astfel încît*

$$\alpha\frac{x}{\log x}<\pi(x)<\beta\frac{x}{\log x}.$$

Demonstraţie. Avem $\vartheta(x)=\sum\limits_{p\leqslant x}\log p\leqslant\sum\limits_{p\leqslant}\log x=\pi(x)\log x$, deci $ax<\vartheta(x)\leqslant\pi(x)\log x$. Deci cu $\alpha=a$ avem $\alpha\frac{x}{\log x}<\pi(x)$.

Apoi $\vartheta(x)=\sum\limits_{p\leqslant x}\log p\geqslant\sum\limits_{\sqrt{x}<p\leqslant x}\log p\geqslant\sum\limits_{\sqrt{x}<p\leqslant x}\log\sqrt{x}=(\pi(x)-$ $-\pi(\sqrt{x}))\log\sqrt{x}=\frac{1}{2}(\pi(x)-\pi(\sqrt{x}))\log x$. Deci $\pi(x)\log x<2\vartheta(x)+$ $+\pi(\sqrt{x})\log x<2\vartheta(x)+\sqrt{x}\log x=O(x)$, deoarece $\vartheta(x)=O(x)$ şi $\sqrt{x}\log x=$ $=O(x)$. Există deci două constante pozitive C_1 şi C_2 astfel încît $|O(x)|<C_1x$ pentru orice x pentru care $x>C_2$. Deci $\pi(x)\log x=$ $=|\pi(x)\log x|=|O(x)|<C_1x$ pentru orice x pentru care $x>C_2$. Avem deci $\frac{\pi(x)\log x}{x}<C_1$ pentru orice x pentru care $x>C_2$. În intervalul $[2,\ C_2]$ să notăm cu M maximul lui $\frac{\pi(x)\log x}{x}$. Punînd $\beta>\max(C_1,\ M)$ obţinem

$$\frac{\pi(x)\log x}{x}<\beta$$

pentru orice x pentru care $x\geqslant 2$. Deci

$$\alpha\frac{x}{\log x}<\pi(x)<\beta\frac{x}{\log x}$$

pentru orice x pentru care $x\geqslant 2$.

Observaţie. În cele ce urmează vom lua $\beta=1{,}6$. Aceasta vom admite fără demonstraţie.

(7) *Dacă $x\geqslant 2$ atunci $|R(x)|<x$.*

Demonstraţie. Ştim că $\Psi(x)=\sum\limits_{r=1}^{\left[\frac{\log x}{\log 2}\right]}\vartheta\left(x^{\frac{1}{r}}\right)$ deci $\Psi(x)\geqslant\vartheta(x)$. Apoi $\Psi(x)=\sum\limits_{p\leqslant x}\left[\frac{\log x}{\log p}\right]\log p\leqslant\sum\limits_{p\leqslant x}\frac{\log x}{\log p}\log p=\sum\limits_{p\leqslant x}\log x=\pi(x)\log x$. Deci

$$\vartheta(x)\leqslant\Psi(x)\leqslant\pi(x)\log x.$$

Din teorema lui **Cebîșev** rezultă că $\pi(x) < 1{,}6\frac{x}{\log x}$, deci $\pi(x)\log x < 1{,}6x$. Apoi avem $\vartheta(x) > ax$ cu $0<a<1$, deci

$$ax < \Psi(x) < 1{,}6x.$$

Dar $\Psi(x) = x + R(x)$, deci

$$-x < (a-1)x < R(x) < 0{,}6x < x$$

de unde $|R(x)| < x$.

Consecință. *Dacă* $x \geqslant 2$ *atunci* $|R(x)| < \alpha_1 x$ *cu* $\alpha_1 \leqslant 1$.

(8) $R(x) = o(x)$.

Demonstrație. Vom lua în considerație relația

$$|R(x)| \leqslant \frac{1}{\log x} \sum_{1 \leqslant n \leqslant x} \left| R\left(\frac{x}{n}\right)\right| + o(x).$$

Vom scrie această relație sub forma

$$|R(x)| \leqslant \frac{x}{\log x} \sum_{1 \leqslant \frac{x}{n} \leqslant x} \frac{1}{n} \left| \frac{n}{x} R\left(\frac{x}{n}\right)\right| + o(x).$$

Vom lua un număr real $\delta = \frac{\alpha_1}{6}$, unde α_1 este numărul real din consecință. Din cauză că $0 < \alpha_1 \leqslant 1$ rezultă $0 < \delta < 1$. Există deci numerele reale $\rho(\delta) > 1$, $x_0 = x_0(\delta)$, $x_1 = x_1(\delta) \geqslant x_0$, $\rho \geqslant \rho(\delta)$ astfel încît pentru oricare x pentru care $x > x_1$ în intervalul $[x, \rho x]$ să existe y cu $|R(y)| < \delta y$ și pentru orice z din intervalul $[y, ye^{\delta/2}]$ să avem $|R(z)| < 3\delta z$. Putem face ca intervalul $[y, ye^{\delta/2}]$ să fie în întregime cuprins în intervalul $[x, \rho x]$ luîndu-l pe ρ suficient de mare.

Vom lua un număr real x_2 pentru care $x_2 \geqslant x_1$ și pentru x dat vom forma o suită de intervale $[x_2\rho^{i-1}, x_2\rho^i]$ cu $i = 1, \ldots, t$, unde pe t îl determinăm prin aceea că

$$x_2\rho^t \leqslant x < x_2\rho^{t+1}.$$

Este suficient pentru aceasta să luăm

$$t = \left[(\log \rho)^{-1} \log\left(\frac{x}{x_2}\right)\right].$$

Bineînțeles, presupunem că $x > x_1$.

În interiorul fiecărui interval $[x_2\rho^{i-1}, x_2\rho^i]$ se va afla un interval $[y_i, y_ie^{\delta/2}]$ astfel încît pentru fiecare z din acest interval să avem $|R(z)| < 3\frac{\alpha_1}{6} z$ deci $|R(z)| < \frac{\alpha_1}{2} z$.

Intervalul de la 1 la x îl vom desface în intervalele $[1, x_2)$, $[x_2, x]$, iar în intervalul $[x_2, x]$ vom pune în evidență intervalele $[y_i, y_ie^{\delta/2}]$. Pentru $z \in [1, x_2)$ vom pune $|R(z)| < z$, pentru $z \in [x_2, x]$ vom pune $|R(z)| < \alpha_1 z$, iar pentru $z \in [y_i, y_ie^{\delta/2}]$ vom pune $|R(z)| < \frac{\alpha_1}{2} z$.

Deci

$$|R(x)| \leqslant \frac{x}{\log x} \sum_{1 \leqslant \frac{x}{n} < x_2} \frac{1}{n} \left| \frac{n}{x} R\left(\frac{x}{n}\right)\right| + \frac{x}{\log x} \sum_{x_2 \leqslant \frac{x}{n} \leqslant x} \frac{1}{n} \left| \frac{n}{x} R\left(\frac{x}{n}\right)\right| + o(x) \leqslant$$

$$\leqslant \frac{x}{\log x} \sum_{1 \leqslant \frac{x}{n} < x_2} \frac{1}{n} + \frac{x}{\log x} \sum_{x_2 \leqslant \frac{x}{n} \leqslant x} \frac{\alpha_1}{n} -$$

$$- \frac{x}{\log x} \sum_{i=1}^{t} \sum_{y_i \leqslant \frac{x}{n} < y_ie^{\delta/2}} \frac{\alpha_1}{2n} + o(x).$$

Am obținut această evaluare, deoarece pentru cazul $1 \leqslant \frac{x}{n} < x_2$ am pus $\left|R\left(\frac{x}{n}\right)\right| < \frac{x}{n}$, deci $\left|\frac{n}{x} R\left(\frac{x}{n}\right)\right| < 1$; pentru cazul $x_2 \leqslant \frac{x}{n} \leqslant x$ am pus $\left|R\left(\frac{x}{n}\right)\right| < \alpha_1 \frac{x}{n}$, deci $\left|\frac{n}{x} R\left(\frac{x}{n}\right)\right| < \alpha_1$ atîta timp cît $\frac{x}{n} \notin [y_i, y_ie^{\delta/2})$ și am pus $\left|R\left(\frac{x}{n}\right)\right| < \frac{\alpha_1}{2} \frac{x}{n}$, deci $\left|\frac{n}{x} R\left(\frac{x}{n}\right)\right| < \frac{\alpha_1}{2} = \alpha_1 - \frac{\alpha_1}{2}$ dacă avem și $\frac{x}{n} \in [y_i, y_ie^{\delta/2})$.

Avem

$$\frac{x}{\log x}\sum_{1\leqslant \frac{x}{n}<x_2}\frac{1}{n}+\frac{x}{\log x}\sum_{x_2\leqslant \frac{x}{n}\leqslant x}\frac{\alpha_1}{n}=\frac{x}{\log x}\sum_{\frac{x}{x_2}<n\leqslant x}\frac{1}{n}+$$

$$+\frac{\alpha_1 x}{\log x}\sum_{1\leqslant n\leqslant \frac{x}{x_2}}\frac{1}{n}=\frac{x}{\log x}\left(\sum_{1\leqslant n\leqslant x}\frac{1}{n}-\sum_{1\leqslant n\leqslant \frac{x}{x_2}}\frac{1}{n}\right)+\frac{\alpha_1 x}{\log x}\sum_{1<n<\frac{x}{x_2}}\frac{1}{n}=$$

$$=\frac{x}{\log x}\left(\log x+C+O\left(\frac{1}{x}\right)-\log\frac{x}{x_2}-C-O\left(\frac{1}{\frac{x}{x_2}}\right)\right)+$$

$$+\frac{\alpha_1 x}{\log x}\left(\log\frac{x}{x_2}+C+O\left(\frac{1}{\frac{x}{x_2}}\right)\right)=$$

$$=\frac{x}{\log x}\left(\log x_2+O\left(\frac{1}{x}\right)\right)+\frac{\alpha_1 x}{\log x}\left(\log x-\log x_2+C+O\left(\frac{1}{x}\right)\right)=$$

$$=\alpha_1 x+o(x).$$

Apoi

$$\frac{x}{\log x}\sum_{i=1}^{t}\sum_{y_i\leqslant\frac{x}{n}<y_i e^{\delta/2}}\frac{\alpha_1}{2n}=\frac{\alpha_1 x}{2\log x}\sum_{i=1}^{t}\sum_{\frac{x}{y_i e^{\delta/2}}<n\leqslant\frac{x}{y_i}}\frac{1}{n}=$$

$$=\frac{\alpha_1 x}{2\log x}\sum_{i=1}^{t}\left(\sum_{1\leqslant n\leqslant\frac{x}{y_i}}\frac{1}{n}-\sum_{1\leqslant n\leqslant\frac{x}{y_i e^{\delta/2}}}\frac{1}{n}\right)=\frac{\alpha_1 x}{2\log x}\sum_{i=1}^{t}\left(\left(\log\frac{x}{y_i}+\right.\right.$$

$$\left.\left.+C+O\left(\frac{1}{\frac{x}{y_i}}\right)\right)-\log\frac{x}{y_i e^{\delta/2}}-C-O\left(\frac{1}{\frac{x}{y_i e^{\delta/2}}}\right)\right)=$$

$$=\frac{\alpha_1 x}{2\log x}\sum_{i=1}^{t}\left(\frac{\delta}{2}+O\left(\frac{y_i}{x}\right)\right)=\frac{\alpha_1 x\,\delta}{4\log x}t+\frac{\alpha_1 x}{2\log x}\sum_{i=1}^{t}O\left(\frac{y_i}{x}\right)>$$

$$>\frac{\alpha_1 x\delta}{4\log x}\left(-1+(\log\rho)^{-1}\log\left(\frac{x}{x_2}\right)\right)+\frac{\alpha_1 x}{2\log x}\sum_{i=1}^{t}O\left(\frac{y_i}{x}\right).$$

În ultima evaluare am ținut seama de

$$(\log\rho)^{-1}\log\left(\frac{x}{x_2}\right)<t+1.$$

Termenul $\frac{\alpha_1 x\delta}{4\log x}\left(-1+(\log\rho)^{-1}\log\left(\frac{x}{x_2}\right)\right)$ se poate transforma astfel

$$\frac{\alpha_1 x\delta}{4\log x}\left(-1+(\log\rho)^{-1}\log\left(\frac{x}{x_2}\right)\right)=\frac{\alpha_1 x\delta}{4\log x}\left(-1+\frac{\log x-\log x_2}{\log\rho}\right)=$$

$$=\frac{\alpha_1 x\delta}{4\log\rho}-\frac{\alpha_1 x\delta}{4\log x}-\frac{\alpha_1\delta x\log x_2}{4\log x\log\rho}.$$

Putem lua $\rho=e^{\frac{K}{\delta}}$ și deci

$$\frac{\alpha_1\delta x}{4\log\rho}=\frac{\alpha_1\delta x}{4\frac{K}{\delta}}=\frac{\alpha_1\delta^2 x}{4K}=\frac{\alpha_1\left(\frac{\alpha_1}{6}\right)^2 x}{4K}=\frac{\alpha_1^3 x}{144\,K}.$$

Apoi

$$-\frac{\alpha_1\delta x}{4\log x}-\frac{\alpha_1\delta x\log x_2}{4\log x\log\rho}=o(x),$$

deoarece α_1, δ, ρ, x_2 sînt constante.

Am arătat deci că

$$\frac{x}{\log x}\sum_{i=1}^{t}\sum_{y_i\leqslant\frac{x}{n}<y_i e^{\delta/2}}\frac{\alpha_1}{2n}>\frac{\alpha_1^3 x}{144K}+o(x)+\frac{\alpha_1 x}{2\log x}\sum_{i=1}^{t}O\left(\frac{y_i}{x}\right).$$

Să evaluăm și pe $\sum_{i=1}^{t}O\left(\frac{y_i}{x}\right)$. Avînd în vedere că $y_i<x_2\rho^i$, avem $0<\frac{y_i}{x}<\frac{x_2\rho^i}{x}=O\left(\frac{x_2\rho^i}{x}\right)$, deci $\frac{y_i}{x}=O\left(\frac{x_2\rho^i}{x}\right)$. Înseamnă că $O\left(\frac{y_i}{x}\right)=O\left(\frac{x_2}{x}\rho^i\right)$,

Putem deci scrie

$$\sum_{i=1}^{t} O\left(\frac{y_i}{x}\right)=\sum_{i=1}^{t} O\left(\frac{x_2}{x}\rho^i\right)=O\left(\frac{x_2}{x}\sum_{i=1}^{t}\rho^i\right).$$

Ultima egalitate este adevărată din cauză că funcția $\frac{x_2}{x}\rho^i$ este definită pentru orice $i\geqslant 1$. Mai departe avem

$$O\left(\frac{x_2}{x}\sum_{i=1}^{t}\rho^i\right)=O\left(\frac{x_2}{x}\frac{\rho^t\rho-\rho}{\rho-1}\right)=O\left(\frac{x_2}{x}\frac{\rho}{\rho-1}(\rho^t-1)\right).$$

Însă $t\leqslant(\log\rho)^{-1}\log\frac{x}{x_2}$, deci $t\log\rho\leqslant\log\frac{x}{x_2}$, deci $\rho^t\leqslant\frac{x}{x_2}$.

Avem deci

$$0<\frac{x_2}{x}\frac{\rho}{\rho-1}(\rho^t-1)\leqslant\frac{x_2}{x}\frac{\rho}{\rho-1}\left(\frac{x}{x_2}-1\right)=\frac{\rho}{\rho-1}\left(1-\frac{x_2}{x}\right)=$$

$$=O\left(\frac{\rho}{\rho-1}\left(1-\frac{x_2}{x}\right)\right)=O(O(1))=O(1).$$

Rezultă că

$$|R(x)|<\alpha_1\left(1-\frac{\alpha_1^2}{144\,K}\right)+o(x)$$

pentru orice x pentru care $x\geqslant x_2$. Există o constantă C astfel încît fiind dat ε real și pozitiv să avem

$$|o(x)|<\varepsilon x$$

pentru orice x pentru care $x\geqslant C$. Deci $o(x)<\varepsilon x$ pentru $x\geqslant C$. Atunci

$$|R(x)|<\alpha_1\left(1-\frac{\alpha_1^2}{144\,K}\right)x+\varepsilon x$$

pentru orice x pentru care $x\geqslant\max(x_2,\ C)$.

Să determinăm un întreg k astfel încît

$$\alpha_1\left(1-\frac{\alpha_1^2}{144\,K}\right)+\varepsilon<\alpha_1\left(1-\frac{\alpha_1^2}{k}\right).$$

Pentru aceasta trebuie ca $-\frac{\alpha_1^3}{144\,K}+\varepsilon<-\frac{\alpha_1^3}{k}$ sau $\frac{\alpha_1^3(k-144K)}{144Kk}>\varepsilon$. Este suficient să luăm $k>144K$ pentru că atunci putem lua ε astfel încît $\frac{\alpha_1^3(k-144K)}{144Kk}>\varepsilon$ și atunci rezultă constanta C astfel încît pentru orice $x\geqslant\max(x_2,\ C)$ să avem

$$|R(x)|<\alpha_1\left(1-\frac{\alpha_1^2}{k}\right)x.$$

Putem lua $x_3=\max(x_2,\ C)$ și atunci

$$|R(x)|<\alpha_2 x$$

pentru orice $x\geqslant x_3$ cu $\alpha_2=\alpha_1\left(1-\frac{\alpha_1^2}{k}\right)$.

Cu x_3 ne găsim în situația în care ne găseam cu x_1. Deci dacă luăm $x_4\geqslant x_3$, putem repeta tot ce am spus în legătură cu x_2 luînd $\delta=\frac{\alpha_2}{6}$. Raționamentul poate fi continuat indefinit și obținem un șir de $\alpha_1,\ \alpha_2,\ldots,$ și $x_2,\ x_4,\ldots,$ cu

$$\alpha_{n+1}=\alpha_n\left(1-\frac{\alpha_n^2}{k}\right)<\alpha_n\quad(n=1,\ 2,\ldots)$$

astfel încît

$$|R(x)|<\alpha_{n+1}x$$

pentru orice x pentru care $x\geqslant x_{2n+2}$.

Vom arăta prin inducție completă că

$$\alpha_n<\sqrt{\frac{k}{2n}}.$$

Pentru $n=1$ avem $\alpha_1<\sqrt{\frac{k}{2}}$ și acest lucru este evident, deoarece $\alpha_1\leqslant 1$, iar $k>144K>144$ deci $\frac{k}{2}>72$, deci $\sqrt{\frac{k}{2}}>1$.

Admițînd că $\alpha_n<\sqrt{\frac{k}{2n}}$ obținem $\alpha_{n+1}<\sqrt{\frac{k}{2n}}\left(1-\frac{k}{2nk}\right)$, deoarece dacă $f(x)=x\left(1-\frac{x^2}{k}\right)$, atunci $f'(x)=1-\frac{3x^2}{k}>0$ dacă $x<\sqrt{\frac{k}{3}}$.

Pentru $n \geqslant 2$ avem $\alpha_n < \sqrt{\frac{k}{3}}$, $\sqrt{\frac{k}{2n}} < \sqrt{\frac{k}{3}}$, deci din $\alpha_n < \sqrt{\frac{k}{2n}}$ am dedus

$$\alpha_{n+1} < \sqrt{\frac{k}{2n}}\left(1 - \frac{1}{2n}\right),$$

deoarece funcția $f(x)$ este crescătoare pentru $x < \sqrt{\frac{k}{3}}$. Inducția trebuie deci începută pentru $n=2$ și se verifică că $\alpha_2 < \sqrt{\frac{k}{4}}$, deoarece avem $\sqrt{\frac{k}{4}} > \sqrt{36} = 6 > 1$, iar $\alpha_2 < \alpha_1 \leqslant 1$. Apoi

$$\frac{1}{\sqrt{n}}\left(1 - \frac{1}{2n}\right) < \frac{1}{\sqrt{n+1}},$$

deoarece $\frac{1}{n}\left(1 - \frac{1}{2n}\right)^2 < \frac{1}{n+1}$ sau $\frac{n+1}{n}\left(1 - \frac{1}{2n}\right)^2 < 1$ sau $\left(1 + \frac{1}{n}\right)\left(1 - \frac{1}{2n}\right)^2 < 1$ sau $\left(1 + \frac{1}{n}\right)\left(1 - \frac{1}{n} + \frac{1}{4n^2}\right) < 1$ sau $1 - \frac{1}{n^2} + \frac{1}{4n^2} + \frac{1}{4n^3} < 1$ sau $\frac{-3}{4n^2} + \frac{1}{4n^3} < 0$ sau $3 > \frac{1}{n}$ sau $n > \frac{1}{3}$. Deci

$$\alpha_{n+1} < \sqrt{\frac{k}{2(n+1)}}.$$

Dacă vrem ca $\alpha_n < \varepsilon$ este suficient să luăm $\sqrt{\frac{k}{2n}} < \varepsilon$ sau $n > \frac{k}{2\varepsilon^2}$. Punînd $C = x_{2n}$ atunci avem că

$$|R(x)| < \varepsilon x$$

pentru orice x pentru care $x > C$ și deci $R(x) = o(x)$.

15.2. Stabilirea legii asimptotice a distribuției numerelor prime pozitive

Vom stabili că

$$\pi(x) \sim \frac{x}{\log x}.$$

Aceasta este legea asimptotică a distribuției numerelor prime. Aceasta înseamnă că

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1.$$

Legea asimptotică a distribuției numerelor prime se deduce în felul următor:

(1) $\Psi(x) \sim x$.

Demonstrație.

$$\Psi(x) = x + R(x) = x + o(x) = x(1 + o(1)) \text{ deci } \Psi(x) \sim x.$$

(2) $\vartheta(x) \sim \pi(x) \log x$.

Demonstrație. Pe de o parte

$$\vartheta(x) = \sum_{p \leqslant x} \log p \leqslant \sum_{p \leqslant x} \log x = \pi(x) \log x.$$

Pe de altă parte

$$\vartheta(x) = \sum_{p \leqslant x} \log p \geqslant \sum_{x^{1-\delta} < p \leqslant x} \log p > \sum_{x^{1-\delta} < p \leqslant x} \log x^{1-\delta} =$$

$$= (\pi(x) - \pi(x^{1-\delta})) \log x^{1-\delta} = (1-\delta)\{\pi(x) - \pi(x^{1-\delta})\} \log x.$$

Obținem deci

$$\pi(x) \log x \geqslant \vartheta(x) > (1-\delta)\{\pi(x) - \pi(x^{1-\delta})\} \log x,$$

de unde

$$1 \geqslant \frac{\vartheta(x)}{\pi(x) \log x} > (1-\delta) - (1-\delta)\frac{\pi(x^{1-\delta})}{\pi(x)}.$$

Conform teoremei lui Cebîșev rezultă

$$\pi(x^{1-\delta}) < \beta \frac{x^{1-\delta}}{\log x^{1-\delta}}, \quad \alpha \frac{x}{\log x} < \pi(x)$$

deci, prin înmulțire membru cu membru,

$$\alpha \pi(x^{1-\delta}) \frac{x}{\log x} < \beta \pi(x) \frac{x^{1-\delta}}{\log x^{1-\delta}},$$

de unde

$$(1-\delta)\frac{\pi(x^{1-\delta})}{\pi(x)}<\frac{\beta}{\alpha}x^{-\delta} \text{ sau } -\frac{\beta}{\alpha}x^{-\delta}<-(1-\delta)\frac{\pi(x^{1-\delta})}{\pi(x)},$$

deci

$$(1-\delta)-\frac{\beta}{\alpha}x^{-\delta}<(1-\delta)-(1-\delta)\frac{\pi(x^{1-\delta})}{\pi(x)}$$

așa că

$$1\geqslant\frac{\vartheta(x)}{\pi(x)\ \log\ x}>(1-\delta)-\frac{\beta}{\alpha}x^{-\delta}.$$

Vom lua $\delta=\frac{1}{\log\ \log\ x}$, deci $x^{-\delta}=\frac{1}{x^{\frac{1}{\log\log x}}}$ și atunci $\lim_{x\to\infty}x^{-\delta}=0$,

deoarece punînd $y=x^{\frac{1}{\log x\ \log x}}$ obținem $\log\ y=\frac{\log\ x}{\log\log\ x}$, $\lim_{x\to\infty}\log\ y=$

$=\lim_{x\to\infty}\frac{\log\ x}{\log\log\ x}=\lim_{x\to\infty}\frac{\frac{1}{x}}{\frac{1}{x\log x}}=\lim_{x\to\infty}\log x=\infty$. Deci $1\geqslant\lim_{x\to\infty}\frac{\vartheta(x)}{\pi(x)\log\ x}\geqslant$

$\geqslant 1$, deci $\lim_{x\to\infty}\frac{\vartheta\ (x)}{\pi\ (x)\log x}=1$, deci $\vartheta(x)\sim\pi(x)\ \log\ x$.

(3) $\pi(x)\sim\frac{x}{\log\ x}$.

Demonstrație.

Avem $\Psi(x)=\vartheta(x)+o(x)$ deci $\Psi(x)\sim\vartheta(x)$. Apoi $\vartheta(x)\sim\pi(x)\log x$, deci $\Psi(x)\sim\pi(x)\log x$ și $\Psi(x)\sim x$ deci $x\sim\pi(x)\log x$ deci $\pi(x)\sim\frac{x}{\log\ x}$.

Capitolul 16

TEOREMA LUI DIRICHLET

16.1. Evaluări asimptotice ale unor sume în care intervin caractere modulo m

Vom considera sume de forma

$$\sum_{v\leqslant n\leqslant x}f(n)\chi(n),$$

unde suma este extinsă la toate numerele naturale n, diferite două cîte două, cuprinse între două numere reale v și x, pentru care $v\leqslant x$, $f(u)$ fiind o funcție reală de variabilă reală u, iar χ fiind caracter modulo m, diferit de caracterul principal. În cazul cînd $\chi\ (n)$ este înlocuit cu 1, sume de acest gen au fost evaluate în paragraful 13.4.

În legătură cu sumele de mai sus avem următoarea teoremă.

Teoremă *Dacă χ nu este caracter principal modulo m, iar $f(u)$ este o funcție pentru care există un număr real C astfel încît $f(u)$ să fie descrescătoare și pozitivă pe intervalul $[C,\ +\infty)$, atunci*

$$\sum_{n>x}f(n)\chi(n)=O(f(x)),$$

unde suma este extinsă la toate numerele naturale n, diferite două cîte două, mai mari ca un număr real pozitiv x.

Demonstrație. Vom nota $n_1=[x]+1$, iar numerele întregi consecutive care urmează după n_1, le vom nota cu $n_2, n_3, \ldots$ În aceste condiții putem scrie

$$\sum_{n>x} f(n)\chi(n)=\sum_{i=1}^{\infty} f(n_i)\chi(n_i).$$

O sumă parțială a acestei serii este

$$\sum_{i=1}^{t} f(n_i)\chi(n_i).$$

Dacă vom pune $a_i=\chi(n_i)$, $b_i=f(n_i)$ vom obține, conform formulei de transformare a sumelor a lui Abel,

$$\sum_{i=1}^{t} f(n_i)\chi(n_i)=\sum_{k=1}^{t} s_k(f(n_k)-f(n_{k+1}))+f(n_{t+1})s_t,$$

unde $s_j=\sum_{l=1}^{j}\chi(n_l)$. Putem scrie $j=mq+r$, $0\leqslant r<|m|$, conform teoremei împărțirii întregi, și atunci

$$s_j=\sum_{l=1}^{j}\chi(n_l)=\sum_{l=1}^{m}\chi(n_l)+\sum_{l=m+1}^{2m}\chi(n_l)+\ldots$$

$$+\sum_{l=(q-1)m+1}^{qm}\chi(n_l)+\sum_{l=qm+1}^{qm+r}\chi(n_l).$$

Dar

$$\sum_{l=1}^{m}\chi(n_l)=\sum_{l=m+1}^{2m}\chi(n_l)=\ldots=\sum_{l=(q-1)m+1}^{qm}\chi(n_l)=0,$$

deoarece fiecare din aceste sume este extinsă la cîte un sistem complet de resturi modulo m. Așadar

$$s_j=\sum_{l=1}^{j}\chi(n_l)=\sum_{l=qm+1}^{qm+r}\chi(n_l).$$

De aici rezultă că

$$|s_j|=\left|\sum_{l=qm+1}^{qm+r}\chi(n_l)\right|\leqslant\sum_{l=qm+1}^{qm+r}\left|\chi(n_l)\right|\leqslant r<|m|.$$

Pe intervalul $[C, +\infty)$ funcția $f(x)$ este descrescătoare și pozitivă deci $f(n_k)-f(n_{k+1})\geqslant 0$ și $f(n_{k+1})>0$ dacă $x>C$ și atunci

$$\left|\sum_{i=1}^{t} f(n_i)\chi(n_i)\right|\leqslant\sum_{k=1}^{t}|s_k|(f(n_k)-f(n_{k+1}))+f(n_{t+1})|s_t|<$$

$$<\sum_{k=1}^{t}|m|(f(n_k)-f(n_{k+1}))+f(n_{t+1})|m|=|m|f(n_1)\leqslant|m|f(x),$$

deci și

$$f(x)>0,\quad\left|\sum_{n>x} f(n)\chi(n)\right|<|m|f(x),$$

pentru orice x pentru care $x>C$, deci teorema este demonstrată.

Din teorema demonstrată mai sus rezultă următoarea teoremă.

Teoremă. *Dacă χ nu este caracter principal modulo m, iar $f(u)$ este o funcție pentru care există un număr real C astfel încît $f(u)$ să fie descrescătoare pozitivă pe intervalul $[C, +\infty)$ și $\lim_{u\to\infty} f(u)=0$, atunci seria*

$$\sum_{n=1}^{\infty} f(n)\chi(n)$$

este convergentă, iar

$$\sum_{1\leqslant n\leqslant x} f(n)\chi(n)=\sum_{n=1}^{\infty} f(n)\chi(n)+O(f(x)).$$

Demonstrație. Datorită teoremei precedente, există două constante pozitive C_1 și C_2, în treacăt fie zis $C_1=|m|$, $C_2=C$ ceea ce rezultă din demonstrația teoremei precedente, astfel încît

$$\left|\sum_{n>x} f(n)\chi(n)\right|<C_1 f(x)$$

pentru orice x pentru care $x>C_2$. Deci

$$\lim_{x\to\infty}\left|\sum_{n>x} f(n)\chi(n)\right|\leqslant C_1\lim_{x\to\infty} f(x)=0.$$

Dar $\sum_{n>x} f(n)\chi(n)$ este restul seriei considerate și cum condiția necesară și suficientă ca o serie să fie convergentă este ca restul

seriei respective să tindă la zero înseamnă că seria considerată este convergentă. Apoi din

$$\sum_{n=1}^{\infty} f(n)\chi(n) = \sum_{1\leqslant n\leqslant x} f(n)\chi(n) + \sum_{n>x} f(n)\chi(n)$$

rezultă

$$\sum_{1\leqslant n\leqslant x} f(n)\chi(n) = \sum_{n=1}^{\infty} f(n)\chi(n) - \sum_{n>x} f(n)\chi(n).$$

Transformînd ultimul termen cu ajutorul teoremei precedente, obținem teorema de față.

Exemple.

(1) Am văzut în exemplul (1) din paragraful 13.4 că funcția $f(u)=\frac{1}{u}$ este descrescătoare pozitivă pe intervalul $[1, +\infty)$. Se mai observă că $\lim_{u\to\infty} f(u)=0$. Deci dacă facem notația

$$L_0(\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n}$$

atunci

$$\sum_{1\leqslant n\leqslant x} \frac{\chi(n)}{n} = L_0(\chi) + O\left(\frac{1}{x}\right).$$

(2) Am văzut în exemplul (4) din paragraful 13.4 că funcția $f(u)=\frac{\log u}{u}$ este descrescătoare pozitivă pe intervalul $[e, +\infty)$. Se mai observă că $\lim_{u\to\infty} f(u)=0$. Deci dacă facem notația

$$L_1(\chi) = \sum_{n=1} \frac{\chi(n)\log n}{n}$$

atunci

$$\sum_{1\leqslant n\leqslant x} \frac{\chi(n)\log n}{n} = L_1(\chi) + O\left(\frac{\log x}{x}\right).$$

(3) Am văzut în exemplul (2) din paragraful 13.4 că funcția $f(u)=\frac{1}{\sqrt{u}}$ este descrescătoare pozitivă pe intervalul $[1, +\infty)$, deoarece

funcția $f(u)=\frac{1}{\sqrt{u}}$ corespunde în exemplul (2) din paragraful 13.4 la $\rho=-\frac{1}{2}$. Se mai observă că $\lim_{u\to\infty} f(u)=0$. Deci dacă facem notația

$$L_2(\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{\sqrt{n}}$$

atunci

$$\sum_{1\leqslant n\leqslant x} \frac{\chi(n)}{\sqrt{n}} = L_2(\chi) + O\left(\frac{1}{\sqrt{x}}\right)$$

16.2. Cîteva proprietăți în legătură cu seriile $L_0(\chi)$, $L_1(\chi)$, $L_2(\chi)$

Teoremă. *Dacă χ este un caracter real modulo m, atunci $L_0(\chi)\neq 0$.*

Demonstrație. Vom considera funcția de sumare a funcției χ, cu alte cuvinte vom lua

$$F(n) = \sum_{d|n} \chi(d),$$

suma fiind extinsă la toți divizorii pozitivi ai lui n, unde n este un număr natural. Caracterul χ fiind o funcție total multiplicativă, funcția sa de sumare $F(n)$ va fi multiplicativă. Din această cauză, dacă descompunem pe n într-un produs de factori primi sub forma

$$n = \prod_{i=1}^{r} p_i^{\alpha_i},$$

unde numerele prime $p_1, p_2, \ldots, p_r$ sînt neasociate două cîte două, obținem

$$F(n) = \prod_{i=1}^{r} F(p_i^{\alpha_i}) = \left(\sum_{\delta_1=0}^{\alpha_1} \chi(p_1^{\delta_1})\right) \ldots \left(\sum_{\delta_r=0}^{\alpha_r} \chi(p_r^{\delta_r})\right).$$

Să examinăm suma

$$\sum_{\delta_i=0}^{\alpha_i} \chi(p_i^{\delta_i}).$$

Dacă p_i nu este prim cu modulul m, atunci nici $p_i^{\delta_i}$ nu va fi prim cu modulul m, pentru $\delta_i \geqslant 1$, deci pentru aceste valori ale lui δ_i avem $\chi(p^{\delta_i})=0$. Aşadar, în acest caz

$$\sum_{\delta_i=0}^{\alpha_i} \chi(p_i^{\delta_i}) = \chi(p_i^0) = \chi(1) = 1.$$

Dacă, însă, p_i este prim cu modulul m, atunci, caracterul χ fiind real, rezultă că $\chi(p_i)=\pm 1$. În acest caz, avem

$$\sum_{\delta_i=0}^{\alpha_i} \chi(p_i^{\delta_i}) = \sum_{\delta_i=0}^{\alpha_i} (\chi(p_i))^{\delta_i} = 1+(\pm 1)+(\pm 1)^2+\ldots+(\pm 1)^{\alpha_i} \geqslant 0$$

Dacă α_i este par rezultă chiar că $\sum_{\delta_i=0}^{\alpha_i} \chi(p_i^{\delta_i}) \geqslant 1$, ceea ce se vede din cele de mai sus. Asta înseamnă că $F(n)\geqslant 0$ şi că $F(k^2)\geqslant 1$ În concluzie, seria

$$G = \sum_{n=1}^{\infty} \frac{F(n)}{\sqrt{n}}$$

este divergentă, deoarece

$$G = \sum_{n=1}^{\infty} \frac{F(n)}{\sqrt{n}} \geqslant \sum_{k=1}^{\infty} \frac{F(k^2)}{\sqrt{k^2}} = \sum_{k=1}^{\infty} \frac{F(k^2)}{k} \geqslant \sum_{k=1}^{\infty} \frac{1}{k}$$

ultima serie fiind seria armonică, care este divergentă.

Pentru a demonstra teorema, vom presupune prin absurd că $L_0(\chi)=0$ şi vom demonstra că seria G este convergentă dacă $L_0(\chi)=0$.

Acest lucru îl vom face considerînd funcţia

$$G(x) = \sum_{1\leqslant n\leqslant x} \frac{F(n)}{\sqrt{n}}$$

care este o sumă parţială a seriei de mai sus.

Avem

$$G(x) = \sum_{1\leqslant n\leqslant x} \frac{1}{\sqrt{n}} \left(\sum_{d|n} \chi(d)\right) = \sum_{1\leqslant n\leqslant x} \left(\sum_{d|n} \frac{\chi(d)}{\sqrt{n}}\right) =$$

$$= \sum_{1\leqslant d\leqslant x} \left(\sum_{1\leqslant d'\leqslant \frac{x}{d}} \frac{1}{\sqrt{dd'}} \chi(d)\right) = \sum_{1\leqslant d\leqslant \sqrt{x}} \left(\sum_{1\leqslant d'\leqslant \frac{x}{d}} \frac{1}{\sqrt{dd'}} \chi(d)\right) +$$

$$+ \sum_{\sqrt{x}<d\leqslant x} \left(\sum_{1\leqslant d'\leqslant \frac{x}{d}} \frac{1}{\sqrt{dd'}} \chi(d)\right) = \sum_{1\leqslant d<\sqrt{x}} \frac{\chi(d)}{\sqrt{d}} \left(\sum_{1\leqslant d'\leqslant \frac{x}{d}} \frac{1}{\sqrt{d'}}\right) +$$

$$+ \sum_{1\leqslant d'<\sqrt{x}} \left(\sum_{\sqrt{x}<d\leqslant \frac{x}{d'}} \frac{\chi(d)}{\sqrt{dd'}}\right).$$

Ultima sumă a fost transformată pentru următorul motiv. Fie M mulţimea tuturor perechilor $(d,\ d')$, unde $\sqrt{x}<d\leqslant x$, $1\leqslant d'\leqslant \frac{x}{d}$, şi fie N mulţimea tuturor perechilor $(d,\ d')$, unde $1\leqslant d'<\sqrt{x}$, $\sqrt{x}<d\leqslant \frac{x}{d'}$. Să arătăm că $M=N$. Într-adevăr, fie $(d,\ d')\in M$. Atunci $\sqrt{x}<d\leqslant x$, $1\leqslant d'\leqslant \frac{x}{d}$, deci $1\leqslant d'\leqslant \frac{x}{d}<\frac{x}{\sqrt{x}}=\sqrt{x}$, adică $1\leqslant d'<\sqrt{x}$, iar din $\sqrt{x}<d$ şi $d'\leqslant \frac{x}{d}$ rezultă $\sqrt{x}<d\leqslant \frac{x}{d'}$. Deci $(d,\ d')\in N$. Reciproc, dacă $(d,\ d')\in N$ avem $1\leqslant d'<\sqrt{x}$, $\sqrt{x}<d\leqslant \frac{x}{d'}$, deci $\sqrt{x}<d\leqslant \frac{x}{d'}\leqslant \frac{x}{1}=x$, adică $\sqrt{x}<d\leqslant x$, iar din $1\leqslant d'$ şi $d\leqslant \frac{x}{d'}$, rezultă $1\leqslant d'\leqslant \frac{x}{d}$. Deci $(d,\ d')\in M$. Avem deci $M=N$. Cele două sume pe care le-am transformat, una se face după mulţimea perechilor $(d,\ d')$, fiecare pereche fiind luată o singură dată, care constituie mulţimea M, iar cealaltă se face după mulţimea perechilor $(d,\ d')$, fiecare pereche fiind luată o singură dată, care constituie mulţimea N şi cele două sume sînt deci egale, deoarece $M=N$.

Cu ajutorul formulelor stabilite pînă acum obținem

$$\sum_{1\leqslant d'\leqslant \frac{x}{d}} \frac{1}{\sqrt{d'}} = \sum_{1\leqslant d'\leqslant \frac{x}{d}} d'^{-1-\left(-\frac{1}{2}\right)} = -\left(-\frac{1}{2}\right)^{-1}\left(\frac{x}{d}\right)^{-\left(-\frac{1}{2}\right)} + C + O\left(\left(\frac{x}{d}\right)^{-1-\left(-\frac{1}{2}\right)}\right) = 2\sqrt{\frac{x}{d}} + C + O\left(\sqrt{\frac{d}{x}}\right).$$

$$\sum_{\sqrt{x}<d\leqslant \frac{x}{d'}} \frac{\chi(d)}{\sqrt{d}} = \sum_{1\leqslant d\leqslant \frac{x}{d'}} \frac{\chi(d)}{\sqrt{d}} - \sum_{1\leqslant d\leqslant\sqrt{x}} \frac{\chi(d)}{\sqrt{d}} =$$

$$= L_2(\chi) + O\left(\sqrt{\frac{d'}{x}}\right) - L_2(\chi) - O\left(\frac{1}{\sqrt[4]{x}}\right) = O\left(\sqrt{\frac{d'}{x}}\right) + O\left(\frac{1}{\sqrt[4]{x}}\right).$$

Așadar

$$G(x) = \sum_{1\leqslant d\leqslant\sqrt{x}} \frac{\chi(d)}{\sqrt{d}}\left(2\sqrt{\frac{x}{d}} + C + O\left(\sqrt{\frac{d}{x}}\right)\right) + \sum_{1\leqslant d'<\sqrt{x}} \frac{1}{\sqrt{d'}}\left(O\left(\sqrt{\frac{d'}{x}}\right) + O\left(\frac{1}{\sqrt[4]{x}}\right)\right) = 2\sqrt{x}\sum_{1\leqslant d\leqslant\sqrt{x}} \frac{\chi(d)}{d} + C\sum_{1\leqslant d\leqslant\sqrt{x}} \frac{\chi(d)}{\sqrt{d}} +$$

$$+ \sum_{1\leqslant d\leqslant\sqrt{x}} \frac{\chi(d)}{\sqrt{d}} O\left(\sqrt{\frac{d}{x}}\right) + \sum_{1\leqslant d'<\sqrt{x}} \frac{1}{\sqrt{d'}} O\left(\sqrt{\frac{d'}{x}}\right) + \sum_{1\leqslant d'<\sqrt{x}} \frac{1}{\sqrt{d'}} O\left(\frac{1}{\sqrt[4]{x}}\right).$$

Avem

$$2\sqrt{x}\sum_{1\leqslant d\leqslant\sqrt{x}} \frac{\chi(d)}{d} = 2\sqrt{x}\left(L_0(\chi) + O\left(\frac{1}{\sqrt{x}}\right)\right) = 2\sqrt{x}L_0(\chi) + O(1);$$

$$C\sum_{1\leqslant d\leqslant\sqrt{x}} \frac{\chi(d)}{\sqrt{d}} = C\left(L_2(\chi) + O\left(\frac{1}{\sqrt[4]{x}}\right)\right) = O(1);$$

$$\left|\sum_{1\leqslant d\leqslant\sqrt{x}} \frac{\chi(d)}{\sqrt{d}} O\left(\sqrt{\frac{d}{x}}\right)\right| \leqslant \sum_{1\leqslant d\leqslant\sqrt{x}} \frac{1}{\sqrt{d}} O\left(\sqrt{\frac{d}{x}}\right) = O\left(\sum_{1\leqslant d\leqslant\sqrt{x}} \frac{1}{\sqrt{d}}\sqrt{\frac{d}{x}}\right) =$$

$$= O\left(\sum_{1\leqslant d\leqslant\sqrt{x}} \frac{1}{\sqrt{x}}\right) = O\left(\frac{[\sqrt{x}]}{\sqrt{x}}\right) = O(1).$$

Deci

$$\sum_{1\leqslant d\leqslant\sqrt{x}} \frac{\chi(d)}{d} O\left(\sqrt{\frac{d}{x}}\right) = O(1).$$

$$\sum_{1\leqslant d'<\sqrt{x}} \frac{1}{\sqrt{d'}} O\left(\sqrt{\frac{d'}{x}}\right) = O\left(\sum_{1\leqslant d'\leqslant\sqrt{x}} \frac{1}{\sqrt{d'}}\sqrt{\frac{d'}{x}}\right) = O\left(\sum_{1\leqslant d'\leqslant\sqrt{x}} \frac{1}{\sqrt{x}}\right) =$$

$$= O\left(\frac{[\sqrt{x}]}{\sqrt{x}}\right) = O(1);$$

$$\sum_{1\leqslant d'<\sqrt{x}} \frac{1}{\sqrt{d'}} O\left(\frac{1}{\sqrt[4]{x}}\right) = O\left(\sum_{1\leqslant d'\leqslant\sqrt{x}} \frac{1}{\sqrt{d'}}\frac{1}{\sqrt[4]{x}}\right) = O\left(\frac{1}{\sqrt[4]{x}}\sum_{1\leqslant d'\leqslant\sqrt{x}} \frac{1}{\sqrt{d'}}\right) =$$

$$= O\left(\frac{1}{\sqrt[4]{x}}\left(2\sqrt[4]{x} + C + O\left(\frac{1}{\sqrt[4]{x}}\right)\right)\right) = O\left(2 + \frac{C}{\sqrt[4]{x}} + O\left(\frac{1}{\sqrt{x}}\right)\right) = O(O(1)) = O(1).$$

Deci

$$G(x) = 2\sqrt{x}L_0(\chi) + O(1).$$

Dacă $L_0(\chi) = 0$ rezultă că $G(x) = O(1)$, adică rezultă că $G(x)$ este mărginită în vecinătatea infinitului, ceea ce înseamnă că seria G, considerată mai înainte, este convergentă. Acest lucru este contradictoriu și deci teorema este demonstrată.

Teoremă. *Dacă χ este un caracter modulo m, diferit de caracterul principal, atunci*

$$L_1(\chi)\sum_{1\leqslant n\leqslant x} \frac{\mu(n)\,\chi(n)}{n} = \begin{cases} -\log x + O(1) & \text{dacă } L_0(\chi) = 0; \\ O(1) & \text{dacă } L_0(\chi) \neq 0, \end{cases}$$

suma fiind extinsă la toate numerele naturale mai mici sau cel mult egale cu un număr real $x \geqslant 1$, μ fiind funcția lui Moebius.

Demonstrație. Considerăm funcția

$$g(x) = \sum_{1\leqslant n\leqslant x} \chi(n)\frac{x}{n}\log\frac{x}{n}.$$

Această funcție se prezintă sub forma $g(x)=\sum_{1\leqslant n\leqslant x} P(n)f\left(\frac{x}{n}\right)$, unde $P(n)=\chi(n)$ este o funcție total multiplicativă cu $P(0)=\chi(0)=1$, iar $f(x)=x\log x$ este o funcție definită pentru orice $x\geqslant 1$. Putem aplica formula de inversare a lui Moebius pentru funcțiile reale sau complexe de variabilă reală. Obținem

$$x\log x=\sum_{1\leqslant n\leqslant x}\mu(n)\chi(n)g\left(\frac{x}{n}\right).$$

Dar

$$g(x)=x\sum_{1\leqslant n\leqslant x}\frac{\chi(n)}{n}\left(\log x-\log n\right)=x\log x\left(L_0(\chi)+O\left(\frac{1}{x}\right)\right)-$$

$$-x\left(L_1(\chi)+O\left(\frac{\log x}{x}\right)\right)=x\log x\,L_0(\chi)+O\left(\frac{x\log x}{x}\right)-xL_1(\chi)+O\left(x\frac{\log x}{x}\right).$$

Funcția $g(x)$, astfel definită, o vom utiliza numai în cazul cînd $L_0(\chi)=0$, deci

$$g(x)=-xL_1(\chi)+O(\log x).$$

Rezultă că

$$x\log x=\sum_{1\leqslant n\leqslant x}\mu(n)\chi(n)\left(-\frac{x}{n}L_1(\chi)+O\left(\log\frac{x}{n}\right)\right)=$$

$$=-xL_1(\chi)\sum_{1\leqslant n\leqslant x}\frac{\mu(n)\chi(n)}{n}+\sum_{1\leqslant n\leqslant x}\mu(n)\chi(n)O\left(\log\frac{x}{n}\right).$$

Avem

$$\left|\sum_{1\leqslant n\leqslant x}\mu(n)\chi(n)O\left(\log\frac{x}{n}\right)\right|\leqslant\sum_{1\leqslant n\leqslant x}O\left(\log\frac{x}{n}\right)=O\left(\sum_{1\leqslant n\leqslant x}\log\frac{x}{n}\right)=$$

$$=O\left(\sum_{1\leqslant n\leqslant x}\log x-\sum_{1\leqslant n\leqslant x}\log n\right)=O([x]\log x-x\log x+x+$$

$$+O(\log x))=O(-\{x\}\log x+x+O(\log x))=O(O(x)+O(x)+$$

$$+O(O(x)))=O(x).$$

Așadar

$$\sum_{1\leqslant n\leqslant x}\mu(n)\chi(n)O\left(\log\frac{x}{n}\right)=O(x).$$

Am obținut deci că

$$xL_1(\chi)\sum_{1\leqslant n\leqslant x}\frac{\mu(n)\chi(n)}{n}=-x\log x+O(x),$$

de unde obținem, prin simplificare cu x, relația din enunțul teoremei.

În cazul cînd $L_0(\chi)\neq 0$, vom considera funcția

$$g(x)=\sum_{1\leqslant n\leqslant x}\chi(n)\frac{x}{n}.$$

Și acestei funcții îi putem aplica formula de inversare a lui Moebius pentru funcțiile reale sau complexe de variabilă reală. Obținem

$$x=\sum_{1\leqslant n\leqslant x}\mu(n)\chi(n)g\left(\frac{x}{n}\right).$$

Dar

$$g(x)=x\sum_{1\leqslant n\leqslant x}\frac{\chi(n)}{n}=x\left(L_0(\chi)+O\left(\frac{1}{x}\right)\right)=xL_0(\chi)+O(1).$$

Deci

$$g(x)=xL_0(\chi)+h(x),$$

unde am notat $h(x)=O(1)$. Rezultă că

$$x=\sum_{1\leqslant n\leqslant x}\mu(n)\chi(n)\left(\frac{x}{n}L_0(\chi)+h\left(\frac{x}{n}\right)\right.=xL_0(\chi)\sum_{1\leqslant n\leqslant x}\frac{\mu(n)\chi(n)}{n}+$$

$$+\sum_{1\leqslant n\leqslant x}\mu(n)\chi(n)h\left(\frac{x}{n}\right).$$

Avem

$$\left|\sum_{1\leqslant n\leqslant x}\mu(n)\chi(n)h\left(\frac{x}{n}\right)\right|\leqslant\sum_{1\leqslant n\leqslant x}\left|h\left(\frac{x}{n}\right)\right|=\sum_{1\leqslant n\leqslant x}O(1)=$$

$$=O\Big(\sum_{1\leqslant n\leqslant x}1\Big)=O([x])=O(x),$$

deci

$$\sum_{1\leqslant n\leqslant x}\mu(n)\chi(n)h\left(\frac{x}{n}\right)=O(x).$$

Am obținut, deci,

$$xL_0(\chi)\sum_{1\leqslant n\leqslant x}\frac{\mu(n)\chi(n)}{n}=O(x)+x=O(x).$$

Prin simplificare cu x și amplificare cu $\frac{L_1(\chi)}{L_0(\chi)}$ obținem rezultatul din enunțul teoremei.

Teoremă. *Dacă χ este un caracter modulo m, diferit de caracterul principal, atunci*

$$\sum_{p\leqslant x}\frac{\chi(p)\ \log\ p}{p}=\sum_{1\leqslant n\leqslant x}\frac{\Lambda(n)}{n}\chi(n)+O(1),$$

prima sumă fiind extinsă la toate numerele prime pozitive cel mult egale cu un număr real x, iar a doua sumă fiind extinsă la toate numerele naturale cel mult egale cu același număr real x.

Demonstrație. Avem

$$\sum_{p\leqslant x}\frac{\chi(p)\log\ p}{p}=\sum_{1\leqslant n\leqslant x}\frac{\chi(n)\ \Lambda(n)}{n}-\Big(\sum_{p^2\leqslant x}\frac{\chi(p^2)\ \log\ p}{p^2}+$$

$$+\sum_{p^3\leqslant x}\frac{\chi(p^3)\ \log\ p}{p^3}+\ldots\Big),$$

deoarece $\Lambda(n)=\log\ p$, dacă $n=p^s$ și $\Lambda(n)=0$, dacă $n\neq p^s$, p fiind un număr prim, iar s un număr natural. Apoi

$$\left|\sum_{p^2\leqslant x}\frac{\chi(p^2)\ \log\ p}{p^2}+\sum_{p^3\leqslant x}\frac{\chi(p^3)\ \log\ p}{p^3}+\ldots\right|\leqslant\sum_{p^2\leqslant x}\frac{\log\ p}{p^2}+$$

$$+\sum_{p^3\leqslant x}\frac{\log\ p}{p^3}+\ldots\leqslant\sum_{p\leqslant x}\log\ p\Big(\sum_{s=2}^{\infty}\frac{1}{p^s}\Big)=\sum_{p\leqslant x}\frac{\frac{1}{p^2}}{1-\frac{1}{p}}\log\ p=$$

$$=\sum_{p\leqslant x}\frac{\log\ p}{p(p-1)}.$$

Dar $p-1\geqslant\frac{1}{2}p$, deoarece $2(p-1)\geqslant p$, adică $p\geqslant 2$. Deci

$$\sum_{p\leqslant x}\frac{\log\ p}{p(p-1)}\leqslant 2\sum_{p\leqslant x}\frac{\log\ p}{p^2}\leqslant 2\sum_{1\leqslant n\leqslant x}\frac{\log\ n}{n^2}=2\sum_{1\leqslant n\leqslant x}n^{-2}\log\ n=O(1),$$

deci

$$\sum_{p^2\leqslant x}\frac{\chi(p^2)\ \log\ p}{p^2}+\sum_{p^3\leqslant x}\frac{\chi(p^3)\ \log\ p}{p^3}+\ldots=O(1).$$

Teorema este deci demonstrată.

Teoremă. *Dacă χ este un caracter modulo m, diferit de caracterul principal, atunci*

$$\sum_{1\leqslant n\leqslant x}\frac{\Lambda(n)}{n}\chi(n)=L_1(\chi)\sum_{1\leqslant n\leqslant x}\frac{\mu(n)\ \chi(n)}{n}+O(1),$$

suma fiind extinsă la toate numerele naturale mai mici sau cel mult egale cu un număr real x.

Demonstrație. Utilizînd relația

$$\Lambda(n)=\sum_{d\mid n}\mu(d)\log\frac{n}{d},$$

suma fiind extinsă la toți divizorii pozitivi ai numărului natural n, obținem

$$\sum_{1\leqslant n\leqslant x}\frac{\Lambda(n)}{n}\chi(n)=\sum_{1\leqslant n\leqslant\alpha}\frac{\chi(n)}{n}\left(\sum_{d|n}\mu(d)\log\frac{n}{d}\right).$$

Punînd $n=dd'$, obținem

$$\sum_{1\leqslant n\leqslant x}\frac{\Lambda(n)}{n}\chi(n)=\sum_{1\leqslant d\leqslant x}\frac{\mu(d)\,\chi(d)}{d}\left(\sum_{1\leqslant d'\leqslant\frac{x}{d}}\frac{\log d'}{d'}\chi(d')\right)=$$

$$=\sum_{1\leqslant d\leqslant x}\frac{\mu(d)\,\chi(d)}{d}\left(L_1(\chi)+O\left(\frac{d}{x}\log\frac{x}{d}\right)\right)=L_1(\chi)\sum_{1\leqslant d\leqslant x}\frac{\mu(d)\,\chi(d)}{d}+$$

$$+\sum_{1\leqslant d\leqslant x}\frac{\mu(d)\,\chi(d)}{d}\,O\left(\frac{d}{x}\log\frac{x}{d}\right).$$

Avem

$$\left|\sum_{1\leqslant d\leqslant x}\frac{\mu(d)\,\chi(d)}{d}O\left(\frac{d}{x}\log\frac{x}{d}\right)\right|\leqslant\sum_{1\leqslant d\leqslant x}\frac{1}{d}\,O\left(\frac{d}{x}\log\frac{x}{d}\right)=$$

$$=O\left(\sum_{1\leqslant d\leqslant x}\frac{1}{d}\,\frac{d}{x}\log\frac{x}{d}\right)=O\left(\frac{1}{x}\left(\sum_{1\leqslant d\leqslant x}\log x-\sum_{1\leqslant d\leqslant x}\log d\right)\right)=$$

$$=O\left(\frac{1}{x}\,O(x)\right)=O(1),$$

și deci am demonstrat că

$$\sum_{1\leqslant d\leqslant x}\frac{\mu(d)\,\chi(d)}{d}\,O\left(\frac{d}{x}\log\frac{x}{d}\right)=O(1)$$

și cu aceasta am demonstrat și teorema.

Teoremă. *Dacă χ este un caracter modulo m, diferit de caracterul principal, atunci*

$$\sum_{p\leqslant x}\frac{\chi(p)\,\log p}{p}=\begin{cases}-\log x+O(1)\text{ dacă }L_0(\chi)=0;\\ O(1)\text{ dacă }L_0(\chi)\neq0.\end{cases}$$

suma fiind extinsă la toate numerele prime pozitive cel mult egale cu un număr real x.

Demonstrația rezultă din ultimele trei teoreme.

Teoremă. *Dacă χ este un caracter modulo m, diferit de caracterul principal, atunci $L_0(\chi)\neq0$.*

Demonstrație. Vom considera expresia

$$\sum_{\substack{2\leqslant p\leqslant x\\ p\equiv1(\mathrm{mod}\ m)}}\frac{\log p}{p}.$$

Din cauză că

$$\sum_{\chi}\chi(p)=\begin{cases}\varphi(m)\text{ dacă }p\equiv1\pmod m;\\ 0\text{ dacă }p\not\equiv1\pmod m),\end{cases}$$

putem scrie

$$\sum_{\substack{2\leqslant p\leqslant x\\ p\equiv1\ (\mathrm{mod}\ m)}}\frac{\log p}{p}=\sum_{2\leqslant p\leqslant x}\frac{\log p}{p}\left(\frac{1}{\varphi(m)}\sum_{\chi}\chi(p)\right)=$$

$$=\frac{1}{\varphi(m)}\sum_{\chi}\sum_{2\leqslant p\leqslant x}\frac{\chi(p)\,\log p}{p},$$

deci

$$\varphi(m)\sum_{\substack{2\leqslant p\leqslant x\\ p\equiv1(\mathrm{mod}\ m)}}\frac{\log p}{p}=\sum_{\chi\neq\chi_1}\sum_{p\leqslant x}\frac{\chi(p)\,\log p}{p}+\sum_{\substack{p\leqslant x\\ (p,m)\cong1}}\frac{\log p}{p}.$$

Ultima sumă este extinsă la toate numerele prime care sînt prime cu modulul m. Numerele prime care nu sînt prime cu modulul m sînt acelea care divid pe m. Astfel de numere prime sînt în număr finit. Deci

$$\sum_{\substack{p\leqslant x\\ (p,m)\cong1}}\frac{\log p}{p}=\sum_{p\leqslant x}\frac{\log p}{p}-\sum_{\substack{p\leqslant x\\ (p,m)\cong1}}\frac{\log p}{p},$$

iar

$$\left|\sum_{\substack{p\leqslant x\\(p,m)\neq 1}}\frac{\log p}{p}\right|\leqslant\sum_{\substack{p\leqslant x\\(p,m)\neq 1}}\frac{\log p}{p}=O(1).$$

Obținem deci

$$\varphi(m)\sum_{\substack{2\leqslant p\leqslant x\\ p\equiv 1\ (\mathrm{mod}\ m)}}\frac{\log p}{p}=\sum_{\chi\neq\chi_1}\sum_{p\leqslant x}\frac{\chi(p)\log p}{p}+\sum_{p\leqslant x}\frac{\log p}{p}+O(1).$$

Dacă N este numărul caracterelor χ modulo m, diferite de caracterul principal, pentru care $L_0(\chi)=0$, deoarece pentru aceste caractere avem

$$\sum_{p\leqslant x}\frac{\chi(p)\log p}{p}=-\log x+O(1),$$

rezultă

$$\varphi(m)\sum_{\substack{2\leqslant p\leqslant x\\ p\equiv 1(\mathrm{mod}\ m)}}\frac{\log p}{p}=(1-N)\log x+O(1),$$

deoarece pentru $L_0(\chi)\neq 0$ avem

$$\sum_{p\leqslant x}\frac{\chi(p)\log p}{p}=O(1).$$

În expresia

$$\varphi(m)\sum_{\substack{2\leqslant p\leqslant x\\ p\equiv 1\ (\mathrm{mod}\ m)}}\frac{\log p}{p}$$

toate cantitățile sînt pozitive sau nu există, deci

$$\varphi(m)\sum_{\substack{2\leqslant p\leqslant x\\ p\equiv 1\ (\mathrm{mod}\ m)}}\frac{\log p}{p}\geqslant 0.$$

În schimb, în $(1-N)\log x+O(1)$ avem $N\geqslant 2$, deoarece dacă χ este caracter modulo m, atunci și conjugatul său $\overline{\chi}$ este caracter modulo m. Dacă χ este caracter complex, atunci și conjugatul

său $\overline{\chi}$ este caracter complex și avem $\chi\neq\overline{\chi}$, deoarece din $\chi\neq\overline{\chi}$ ar rezulta că χ este caracter real. Dar $L_0(\chi)=0$ nu poate avea loc decît pentru caractere complexe χ. În acest caz avem și $L_0(\overline{\chi})=0$. Deci $N\geqslant 2$

Datorită faptului că $N\geqslant 2$, vom folosi definiția lui $O(1)$. Există două constante pozitive C_1 și C_2 astfel încît

$$|O(1)|<C_1$$

pentru orice x pentru care $x>C_2$. Deci

$$-C_1<O(1)<C_1$$

pentru orice x pentru care $x>C_2$. Rezultă că

$$(1-N)\log x-C_1<(1-N)\log x+O(1)<(1-N)\log x+C_1.$$

Relația

$$(1-N)\log x+C_1<0$$

este echivalentă cu

$$x>e^{\frac{C_1}{N-1}}.$$

Dacă luăm $x>\max\left(C_2, e^{\frac{C_1}{N-1}}\right)$, atunci

$$(1-N)\log x+O(1)<0$$

ceea ce vine în contradicție cu faptul că pentru orice x avem

$$(1-N)\log x+O(1)=\varphi(m)\sum_{\substack{2\leqslant p\leqslant x\\ p\equiv 1(\mathrm{mod}\ m)}}\frac{\log p}{p}\geqslant 0.$$

Cu aceasta teorema este demonstrată.

Consecință. *Dacă χ este caracter modulo m, diferit de caracterul principal, atunci*

$$\sum_{p\leqslant x}\frac{\chi(p)\log p}{p}=O(1),$$

deoarece $L_0(\chi)\neq 0$.

16.3. Demonstrația teoremei lui Dirichlet

Teorema lui Dirichlet enunțată mai jos ca în paragraful 12.2, o vom demonstra acum cu ajutorul rezultatelor obținute în acest capitol. Înainte de a demonstra teorema lui Dirichlet, vom demonstra următoarea teoremă.

Teoremă.

$$\sum_{\substack{p\leqslant x\\ p\equiv a \pmod m\\ (a,m)\cong 1}} \frac{\log p}{p} = \frac{1}{\varphi(m)} \log x + O(1),$$

suma fiind extinsă la toate numerele prime pozitive p dintr-o clasă de resturi primă cu modulul și mai mici sau cel mult egale cu x, x fiind un număr real.

Demonstrație. Ținînd seama de următoarea proprietate a caracterelor

$$\sum_{\chi} \chi(p)\overline{\chi(a)} = \begin{cases} \varphi(m) \text{ dacă } p\equiv a \pmod m,\ (a,\ m)\cong 1\ ;\\ 0 \text{ dacă } p\not\equiv a \pmod m,\ (a,\ m)\cong 1, \end{cases}$$

obținem că

$$\sum_{\substack{p\leqslant x\\ p\equiv a \pmod m\\ (a,m)\cong 1}} \frac{\log p}{p} = \sum_{\substack{p\leqslant x\\ (a,m)\cong 1}} \frac{\log p}{p}\left(\varphi(m) - \sum_{\chi} \chi(p)\overline{\chi(a)}\right) =$$

$$= \frac{1}{\varphi(m)} \sum_{\substack{\chi\\ (a,m)\cong}} \overline{\chi(a)}\left(\sum_{p\leqslant x} \frac{\chi(p)\ \log p}{p}\right) = \frac{1}{\varphi(m)}\overline{\chi_1(a)} \sum_{p\leqslant x} \frac{\chi_1(p)\log p}{p} +$$

$$+ \frac{1}{\varphi(m)} \sum_{\substack{\chi\neq\chi_1\\ (p,\ m)\cong 1}} \overline{\chi(a)}\left(\sum_{p\leqslant x} \frac{\chi(p)\ \log p}{p}\right).$$

În ultima expresie $\chi_1(a)=1$, deoarece $(a,\ m)\cong 1$, iar în aceste condiții $\overline{\chi_1(a)}=1$. Conform unei teoreme din paragraful 14.4. și unui raționament din demonstrația teormei precedente rezultă că

$$\sum_{p\leqslant x} \frac{\chi_1(p)\ \log p}{p} = \sum_{\substack{p\leqslant x\\ (p,\ m)\cong 1}} \frac{\log p}{p} = \log x + O(1).$$

Apoi

$$\sum_{\chi\neq\chi_1} \overline{\chi(a)}\left(\sum_{p\leqslant x} \frac{\chi(p)\ \log p}{p}\right) = \sum_{\chi\neq\chi_1} \overline{\chi(a)}O(1) = O(1),$$

suma $\sum\limits_{\chi\neq\chi_1} \overline{\chi(a)}O(1)$ avînd un număr finit de termeni. Deci

$$\sum_{\substack{p\leqslant x\\ p\equiv a \pmod m\\ (a,m)\cong 1}} \frac{\log p}{p} = \frac{1}{\varphi(m)}(\log x + O(1)) + \frac{1}{\varphi(m)}\ O\ (1) = \frac{1}{\varphi(m)}\log x + O(1).$$

Demonstrația teoremei lui Dirichlet rezultă din teorema demonstrată. Teorema lui Dirichlet are următorul enunț:

Teoremă. *În orice clasă de resturi primă cu modulul există o infinitate de numere prime.*

Demonstrație. Presupunem, prin absurd, că într-o clasă de resturi primă cu modulul există numai un număr finit de numere prime pozitive sau că nu există nici unul. Atunci pentru orice x pentru care $x>\max(0,\ p_n)$, avem

$$\sum_{\substack{p\leqslant x\\ p\equiv a \pmod m\\ (a,m)\cong 1}} \frac{\log p}{p} = C,$$

unde

$$C = \frac{\log p_1}{p_1} + \frac{\log p_2}{p_2} + \ldots + \frac{\log p_n}{p_n},$$

$p_1,\ p_2, \ldots,\ p_n$ fiind toate numerele prime pozitive, în cazul cînd ele există, din clasa de resturi primă cu modulul considerată, p_n fiind cel mai mare din ele. Am luat $x\geqslant\max(0,\ p_n)$, deoarece dacă nu există numere prime pozitive în clasa de resturi primă cu modulul considerată atunci suma de mai sus rămîne neschimbată, egală cu 0, pentru orice x pentru care $x>0$.

Dar pentru $O(1)$, care intervine în expresia sumei de mai sus, există două constante pozitive C_1 și C_2 astfel încît pentru orice x pentru care $x\geqslant C_2$ să avem

$$-C_1 < O(1) < C_1.$$

Rezultă că pentru orice x pentru care $x \geqslant C_2$ avem

$$\frac{1}{\varphi(m)} \log x - C_1 < \frac{1}{\varphi(m)} \log x + O(1) < \frac{1}{\varphi(m)} \log x + C_1.$$

Avem

$$C < \frac{1}{\varphi(m)} \log x - C_1,$$

dacă

$$x > e^{\varphi(m)(C+C_1)}.$$

Asta înseamnă, că dacă notăm cu p_n pe cel mai mare număr prim pozitiv din clasa de resturi considerată, primă cu modulul, sau dacă punem $p_n = 0$ în cazul cînd nu există numere prime pozitive în clasa de resturi considerată, atunci pentru $x > \max(C_2, p_n, e^{\varphi(m)(C+C_1)})$ obţinem

$$C = \sum_{\substack{p \leqslant x \\ p \equiv a \pmod m \\ (a,m)=1}} \frac{\log p}{p} = \frac{1}{\varphi(m)} \log x + O(1) > C,$$

ceea ce este contradictoriu. Cu aceasta teorema lui Dirichlet este demonstrată.

Observaţie. Din demonstraţia dată rezultă că am demonstrat ceva mai mult decît afirmă teorema lui Dirichlet, anume am demonstrat că în orice clasă de resturi primă cu modulul există o infinitate de numere prime pozitive.

Bibliografie

1. Creangă, I., Cazacu, C., Minuţ, P., Opaiţ, Gh., Reischer, Corina, *Introducere în teoria numerelor*, Editura didactică şi pedagogică, Bucureşti, 1965.
2. Froda, Alex., *Introducere în algebra modernă*, vol. I, (*Teoria mulţimilor*), Editura ştiinţifică, Bucureşti, 1968.
3. Froda, Alex., *Introducere în algebra modernă*, vol. II, (*Structuri algebrice*), Editura enciclopedică română, Bucureşti, 1970.
4. Galbură, Gh., *Algebră*, Editura didactică şi pedagogică, Bucureşti, 1972.
5. Гельфонд, А., О., Линник, Ю., *В., Елементарные методы в аналитической теории чисел*, Москва, 1962.
6. Хассе, Х., *Лекции по теории чисел*, Москва, 1953.
7. Ion, D., Ion, Radu, N., *Algebră*, Editura didactică şi pedagogică, Bucureşti, 1970.
8. Moisil, C., Gr., *Introducere în algebră*, I, Inele şi ideale, Editura Academiei Republicii Socialiste România, Bucureşti, 1954, vol. I.
9. Popovici, P., Constantin, *Aritmetica şi teoria numerelor*, Editura didactică şi pedagogică, Bucureşti, 1963 şi 1970.
10. Popovici, P., Constantin, *Asupra teoremei lui Dirichlet referitoare la infinitatea numerelor prime pozitive de forma* 4k+1 şi 6k+1, Comunicările Academiei Republicii Socialiste România, t. XI, nr. 7, 1961.
11. Эрнст Трост, Простые числа, Москва, 1959.
12. Vinogradov, I., M., *Bazele teoriei numerelor*, Editura Academiei Republicii Socialiste România, Bucureşti, 1954.

Tabla de materii

Prefaţă 3
Simboluri şi notaţii 5

Capitolul 1

Relaţia de congruenţă 9

1.1. Definiţia relaţiei de congruenţă 9
1.1.1. Definiţia inelului 9
1.1.2. Definiţia relaţiei de divizibilitate în inelul numerelor întregi 10
1.1.3. Definiţia relaţiei de asociere în inelul numerelor întregi 11
1.2. Prima definiţie a relaţiei de congruenţă în inelul numerelor întregi 12
1.3. A doua definiţie a relaţiei de congruenţă în inelul numerelor întregi 14
1.4. Utilizarea relaţiei de congruenţă în inelul numerelor întregi la rezolvarea problemelor de divizibilitate 16

Capitolul 2

Rezolvarea congruenţelor şi a sistemelor de congruenţe cu o necunoscută 18
2.1. Rezolvarea congruenţei de gradul întîi cu o necunoscută 18
2.2. Rezolvarea sistemelor de congruenţe de gradul întîi cu o necunoscută 20
2.3. Congruenţe în raport cu un modul prim 23

Capitolul 3

Clase de resturi 27

3.1. Clase de echivalenţă 27
3.2. Clase de resturi *modulo m* 29
3.3. Inelul claselor de resturi modulo *m* 30
3.4. Clase de resturi prime cu modulul 33
3.5. Grupul multiplicativ al claselor de resturi prime cu modulul 34
3.6. Corpul claselor de resturi faţă de un modul prim 36
3.7. Relaţia de congruenţă în inelul numerelor *m*-întregi . . . 37
3.7.1. Relaţia de divizibilitate în inelul numerelor *m*-întregi 39
3.7.2. Relaţia de congruenţă în inelul numerelor *m*-întregi 40
3.7.3. Clase de resturi modulo *m* în inelul numerelor *m*-întregi 42

Capitolul 4

Teoremele lui Euler, Fermat şi Wilson 43

4.1. Sisteme complete de resturi modulo *m* 43
4.2. Sisteme reduse de resturi modulo *m* 45
4.3. Indicatorul lui Euler 48
4.4. Teoremele lui Euler, Fermat şi Wilson 53

Capitolul 5

Rădăcini primitive 58

5.1. Ordinul unei clase de resturi modulo *m*, primă cu modulul 58
5.2. Rădăcini primitive *modulo m* 63
5.3. Existenţa rădăcinilor primitive modulo *m* 68
5.4. Determinarea rădăcinilor primitive *modulo m* 73
5.5. Rădăcini primitive în corpul numerelor complexe pentru ecuaţia binomă 76

Capitolul 6

Indici modulo m 78

6.1. Indici modulo $\pm p^\beta$ şi $\pm 2p^\beta$, unde p este prim pozitiv impar, iar β este număr natural 78
6.2. Consecinţe ale definiţiei indicilor modulo *m* 83

6.3. Rezolvarea congruenței $x^n \equiv a \pmod m$ cu ajutorul indicilor 85
6.4. Indici modulo $\pm 2^\alpha$, α fiind un număr întreg nenegativ . . 88
6.5. Indici în raport cu un modul diferit de zero 93

Capitolul 7

Funcții numerice 96

7.1. Definiția funcțiilor numerice 96
7.2. Partea întreagă și partea fracționară ale unui număr real 100
7.3. Numărul divizorilor pozitivi 104
7.4. Suma divizorilor pozitivi 106

Capitolul 8

Formule de inversare a sumelor 112

8.1. Funcția lui Moebius 112
8.2. Formula de inversare a lui Moebius 114
8.3. Formula de inversare a lui Moebius pentru funcțiile reale sau complexe de variabilă reală 124
8.4. Funcția lui Mangoldt 128
8.5. Funcția $\Psi(x)$ 129

Capitolul 9

Numărul numerelor prime 131

9.1. Funcția $\varphi(x, r)$ 131
9.2. Funcția $\pi(x)$ 135

Capitolul 10

Caractere modulo m 142

10.1. Definiția caractelor modulo m 142
10.2. Cîteva proprietăți ale caracterelor modulo m 145
10.3. Proprietățile caracterelor modulo m în legătură cu sumele care se fac cu ele 149
10.4. Simbolul lui Legendre 151

Capitolul 11

Resturi pătratice 154

11.1. Criterii ca un număr întreg a să fie rest pătratic modulo p, unde p este un număr prim impar 154
11.2. Legea reciprocității pătratice 159

11.3. Calculul simbolurilor lui Legendre $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$, $\left(\frac{-3}{p}\right)$ . . . 162
11.4. Simbolul lui Jacobi 166

Capitolul 12

Infinitatea numerelor prime 172

12.1. Teorema lui Euclid 172
12.2. Teorema lui Dirichlet 173
12.3. Demonstrația teoremei lui Dirichlet în cazul progresiilor aritmetice $-1+k4$ și $-1+k6$ 174
12.4. Demonstrația teoremei lui Dirichlet în cazul progresiilor aritmetice $1+k4$ și $1+k6$ cu ajutorul resturilor pătratice 177
12.5. Demonstrația teoremei lui Dirichlet în cazul progresiilor aritmetice $1+k4$ și $1+k6$ fără ajutorul resturilor pătratice 179

Capitolul 13

Comportare asimptotică 184

13.1. Comportarea asimptotică a funcțiilor reale sau complexe de variabilă reală 184
13.2. Cîteva proprietăți ale comportării asimptotice 189
13.3. Cazuri particulare de comportare asimptotică 193
13.4. Evaluarea asimptotică a unor sume 202

Capitolul 14

Evaluări asimptotice ale cîtorva funcții numerice 213

14.1. Evaluarea asimptotică a funcției $\Psi(x)$ 213
14.2. Evaluări asimptotice ale unor sume în care intervine funcția lui Mangoldt 216
14.3. Evaluări asimptotice ale funcției $\pi(x)$ 237
14.4. Funcția $\vartheta(x)$ 241

Capitolul 15

Legea asimptotică a distribuției numerelor prime 249

15.1. Funcția $R(x)$ 249
15.2. Stabilirea legii asimptotice a distribuției numerelor prime pozitive 268

Capitolul 16

Teorema lui Dirichlet 271

16.1. Evaluări asimptotice ale unor sume în care intervin caractere modulo m 271

16.2. Cîteva proprietăţi în legătură cu seriile $L_0(\chi)$, $L_1(\chi)$, $L_2(\chi)$ 275

16.3. Demonstraţia teoremei lui Dirichlet 288

Bibliografie 291

Coli de tipar : 18,500
Tiraj : 5 200+120 leg. 1/2
Apărut 1973

I. P. „Oltenia" Craiova
Str. Mihai Viteazul nr. 4
Republica Socialistă România
Pl. 5241/109